

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 1 9 日
Date of Application:

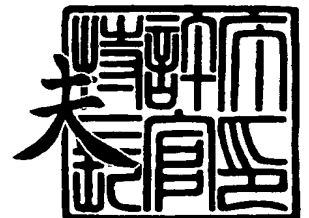
出 願 番 号 特 願 2 0 0 3 - 0 7 4 7 8 1
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 7 4 7 8 1]

出 願 人 日 本 電 気 株 式 会 社
Applicant(s):

2 0 0 3 年 8 月 2 0 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 35001197

【特記事項】 特許法第 3 0 条第 1 項の規定の適用を受けようとする特
許出願

【提出日】 平成15年 3月19日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/22
G06F 13/00

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 中江 政行

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100097157

【弁理士】

【氏名又は名称】 桂木 雄二

【先の出願に基づく優先権主張】

【出願番号】 特願2002-238989

【出願日】 平成14年 8月20日

【手数料の表示】

【予納台帳番号】 024431

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9303562

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 攻撃防御システムおよび攻撃防御方法

【特許請求の範囲】

【請求項 1】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、前記おとり装置は、

前記ファイアウォール装置から転送された入力 IP パケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有し、

前記ファイアウォール装置は、

入力 IP パケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力 IP パケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力 IP パケットのヘッダ情報および振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

前記おとり装置へ転送した入力 IP パケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて、当該入力 IP パケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有することを特徴とする攻撃防御システム。

【請求項 2】 入力 IP パケットの前記ヘッダ情報は当該入力 IP パケットの送信元 IP アドレスおよび宛先 IP アドレスの少なくとも一方であり、

前記転送先選択手段は前記入力 IP パケットのヘッダ情報が前記振り分け条件を満たすか否かに依存して当該入力 IP パケットの転送先を決定する、

ことを特徴とする請求項 1 記載の攻撃防御システム。

【請求項 3】 前記転送先選択手段は、

前記内部ネットワークで使用されていない IP アドレスからなる誘導リストを前記振り分け条件として保持する格納手段を有し、

前記入力 IP パケットの宛先 IP アドレスと前記誘導リスト内の未使用 IP アドレスとが一致したときに当該入力 IP パケットを前記おとり装置へ転送する、

ことを特徴とする請求項 1 記載の攻撃防御システム。

【請求項4】 前記ファイアウォール装置は、前記おとり装置へ転送した入力IPパケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて、前記振り分け条件を更新する振り分け条件更新手段をさらに有することを特徴とする請求項1記載の攻撃防御システム。

【請求項5】 前記フィルタリング条件管理手段は、前記おとり装置へ転送した入力IPパケットのヘッダ情報に対応するフィルタリング条件を有効期限と共に設定し、前記入力IPパケットに対応するフィルタリング条件の有効期限が超過している場合には、デフォルトのフィルタリング条件を前記パケットフィルタリング手段へ返すことを特徴とする請求項1記載の攻撃防御システム。

【請求項6】 前記フィルタリング条件管理手段は、
前記攻撃検知手段が攻撃を検知した際の攻撃カテゴリと当該入力IPパケットのアドレス情報とに対応したフィルタリング条件を生成する条件生成手段と、
前記条件生成手段により生成されたフィルタリング条件に従って、フィルタリング条件を動的に更新するためのフィルタリング条件制御手段と、
を有することを特徴とする請求項1ないし5のいずれかに記載の攻撃防御システム。

【請求項7】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、
前記ファイアウォール装置は、
入力IPパケットのヘッダ情報および振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記転送先選択手段は、前記入力IPパケットの送信元IPアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力IPパケットの転送先を決定することを特徴とする攻撃防御システム。

【請求項 8】 前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度を更新することを特徴とする請求項 7 記載の攻撃防御システム。

【請求項 9】 前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度に所定数を加算することを特徴とする請求項 8 記載の攻撃防御システム。

【請求項 10】 前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度に対応する入力 IP パケットのパケットサイズが大きくなるほど値が小さくなる変数を、当該信頼度に加算することを特徴とする請求項 8 記載の攻撃防御システム。

【請求項 11】 前記信頼度管理手段は、前記入力 IP パケットが予め定められたプロトコルのパケットである場合のみ信頼度の更新を実行することを特徴とする請求項 8 記載の攻撃防御システム。

【請求項 12】 前記信頼度管理手段は、
複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度と当該信頼度の最終更新時刻とを格納するための第 1 信頼度格納手段と、

前記第 1 信頼度格納手段の内容の複製を格納するための第 2 信頼度格納手段と、

前記信頼度格納手段に格納されたある信頼度が前記転送先選択手段によって取得されるごとに、当該信頼度を更新する第 1 更新処理手段と、

前記第 1 信頼度格納手段の内容を定期的に複製して前記第 2 信頼度格納手段へ格納するための複製処理手段と、

前記第 2 信頼度格納手段に格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を更新する第 2 更新処理手段と、

を有することを特徴とする請求項 7 記載の攻撃防御システム。

【請求項 13】 前記複製処理手段は、前記第 1 信頼度格納手段に格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を有するエントリを前記第 1 信頼度格納手段から削除することを特徴とする請求項 12 記載の攻撃防御システム。

【請求項 14】 前記第 2 更新処理手段は、前記最終更新時刻から所定期間

が経過した信頼度を所定値だけ低下させることを特徴とする請求項 12 記載の攻撃防御システム。

【請求項 15】 前記第 2 更新処理手段は、前記最終更新時刻から所定期間が経過した信頼度を前記第 2 更新処理手段から削除することを特徴とする請求項 12 記載の攻撃防御システム。

【請求項 16】 前記おとり装置は、前記ファイアウォール装置から転送された入力 IP パケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有することを特徴とする請求項 7 記載の攻撃防御システム。

【請求項 17】 前記信頼度管理手段は、前記おとり装置へ転送した入力 IP パケットに関して前記攻撃検知手段が攻撃を検知したか否かに応じて、当該入力 IP パケットの送信元 IP アドレスの信頼度を更新することを特徴とする請求項 16 記載の攻撃防御システム。

【請求項 18】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、前記ファイアウォール装置は、
第 1 転送先選択手段と、
第 2 転送先選択手段と、
複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を管理するための信頼度管理手段と、
を有し、

前記第 1 転送先選択手段は、入力 IP パケットのヘッダ情報および第 1 所定条件に基づいて、当該入力 IP パケットを前記第 2 転送先選択手段および前記おとり装置のいずれかへ転送し、

前記第 2 転送先選択手段は、前記第 1 転送先選択手段から転送された前記入力 IP パケットの送信元 IP アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が第 2 所定条件を満たすか否かに応じて当該入力 IP パケットの転送先を前記内部ネットワーク及び前記おとり装置のいずれかに決定する、
ことを特徴とする攻撃防御システム。

【請求項 19】 内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御方法において、

IP パケットのフィルタリング条件および振り分け条件を用意し、

入力 IP パケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力 IP パケットを受理するか否かを判定し、

受理された入力 IP パケットのヘッダ情報および前記振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力 IP パケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力 IP パケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御方法。

【請求項 20】 入力 IP パケットの前記ヘッダ情報は当該入力 IP パケットの送信元 IP アドレスおよび宛先 IP アドレスの少なくとも一方であり、

前記入力 IP パケットのヘッダ情報が前記振り分け条件を満たすか否かに依存して当該入力 IP パケットの転送先を決定することを特徴とする請求項 19 記載の攻撃防御方法。

【請求項 21】 前記振り分け条件は、前記内部ネットワークで使用されていない IP アドレスからなる誘導リストであり、

前記入力 IP パケットの宛先 IP アドレスと前記誘導リスト内の未使用 IP アドレスとが一致したときに当該入力 IP パケットを前記おとり装置へ転送することを特徴とする請求項 19 記載の攻撃防御方法。

【請求項 22】 攻撃を検知したか否かに基づいて、前記振り分け条件を更新するステップをさらに有することを特徴とする請求項 19 記載の攻撃防御方法。

【請求項 23】 前記フィルタリング条件管理ステップは、

前記おとり装置へ転送した入力 IP パケットのヘッダ情報に対応するフィルタリング条件を有効期限と共に設定し、

前記入力 IP パケットに対応するフィルタリング条件の有効期限が超過している場合には、デフォルトのフィルタリング条件を設定する、
ことを特徴とする請求項 19 記載の攻撃防御方法。

【請求項 24】 前記フィルタリング条件管理ステップは、
攻撃を検知した際の攻撃カテゴリと当該入力 IP パケットのアドレス情報とに対応したフィルタリング条件を生成し、
生成されたフィルタリング条件に従って、フィルタリング条件を動的に更新する、
ことを特徴とする請求項 19 記載の攻撃防御方法。

【請求項 25】 内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御方法において、
IP パケットの振り分け条件を用意し、
複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を保持し、
入力 IP パケットの送信元 IP アドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、
ステップを有することを特徴とする攻撃防御方法。

【請求項 26】 前記信頼度を保持するステップは、
複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度と当該信頼度の最終更新時刻とをリアルタイム信頼度データベースに格納し、
前記リアルタイム信頼度データベースに格納されたある信頼度がアクセスされるごとに当該信頼度を更新し、
前記リアルタイム信頼度データベースの内容を定期的に複製して長期信頼度データベースに格納し、
前記長期信頼度データベースに格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を更新する、
ステップを有することを特徴とする請求項 25 記載の攻撃防御方法。

【請求項 27】 前記おとり装置において、前記ファイアウォール装置から転送された入力 IP パケットに対するサービスプロセスを実行することで攻撃の

有無を検知するステップをさらに有することを特徴とする請求項 25 記載の攻撃防御方法。

【請求項 28】 攻撃が検知されたか否かに応じて、当該入力 IP パケットの送信元 IP アドレスの信頼度を更新するステップをさらに有することを特徴とする請求項 27 記載の攻撃防御方法。

【請求項 29】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

入力 IP パケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力 IP パケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力 IP パケットのヘッダ情報および振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

前記おとり装置へ転送した入力 IP パケットに関して前記おとり装置が攻撃を検知したか否かに基づいて、当該入力 IP パケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有することを特徴とするファイアウォール装置。

【請求項 30】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

入力 IP パケットのヘッダ情報および振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記転送先選択手段は、前記入力 IP パケットの送信元 IP アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力 IP パケットの転送先を決定することを特徴とするファイアウォール装置。

【請求項 31】 内部ネットワークと外部ネットワークとの境界に設置され

、おとり装置に接続されたファイアウォール装置において、

第1転送先選択手段と、

第2転送先選択手段と、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記第1転送先選択手段は、入力IPパケットのヘッダ情報および第1所定条件に基づいて、当該入力IPパケットを前記第2転送先選択手段および前記おとり装置のいずれかへ転送し、

前記第2転送先選択手段は、前記第1転送先選択手段から転送された前記入力IPパケットの送信元IPアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が第2所定条件を満たすか否かに応じて当該入力IPパケットの転送先を前記内部ネットワーク及び前記おとり装置のいずれかに決定することを特徴とするファイアウォール装置。

【請求項32】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

入力IPパケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力IPパケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力IPパケットのヘッダ情報および振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を管理するための信頼度管理手段と、

前記おとり装置へ転送した入力IPパケットに関して前記おとり装置が攻撃を検知したか否かに基づいて、当該入力IPパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有し、

前記転送先選択手段は、前記入力IPパケットの送信元IPアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満た

すか否かに応じて当該入力 IP パケットの転送先を決定することを特徴とするファイアウォール装置。

【請求項 33】 前記おとり装置および前記ファイアウォール装置は単一ユニットに收容されていることを特徴とする請求項 1、7 および 18 のいずれかに記載の攻撃防御システム。

【請求項 34】 前記転送先選択手段は、
入力 IP パケットを格納するパケットバッファと、
前記入力 IP パケットを前記内部ネットワークに転送し、宛先到達不能メッセージを受信するか否かを監視する監視手段と、
を有し、
前記監視手段が宛先到達不能メッセージを受信した場合、対応する入力 IP パケットを前記パケットバッファから前記おとり装置へ転送することを特徴とする請求項 1 記載の攻撃防御システム。

【請求項 35】 コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御システムを実装するためのプログラムにおいて、

IP パケットのフィルタリング条件および振り分け条件を用意し、
入力 IP パケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力 IP パケットを受理するか否かを判定し、
受理された入力 IP パケットのヘッダ情報および前記振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力 IP パケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力 IP パケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御プログラム。

【請求項 36】 コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御

システムを実装するためのプログラムにおいて、

IPパケットの振り分け条件を用意し、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を保持し、

入力IPパケットの送信元IPアドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とする攻撃防御プログラム。

【請求項 37】 コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたおとり装置を用いたファイアウォール装置を実装するためのプログラムにおいて、

IPパケットのフィルタリング条件および振り分け条件を用意し、

入力IPパケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力IPパケットを受理するか否かを判定し、

受理された入力IPパケットのヘッダ情報および前記振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に対して、転送した入力IPパケットに対するサービスプロセスを実行させることで攻撃の有無を検知させ、前記おとり装置が攻撃を検知したか否かに基づいて、当該入力IPパケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とするプログラム。

【請求項 38】 コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたおとり装置を用いたファイアウォール装置を実装するためのプログラムにおいて、

IPパケットの振り分け条件を用意し、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を保持し、

入力IPパケットの送信元IPアドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とするプログラム。

【請求項 39】 攻撃防御システムのおとり装置において、

サービスプロセスの実行において、少なくともネットワーク入出力、ファイル入出力、および、プロセス生滅に係るイベントを一時的に記憶するイベント記憶手段と、

前記イベント記憶手段に記憶されたイベント間の因果関係を分析して、リンク付けを行うイベント管理手段と、

を有することを特徴とするおとり装置。

【請求項 40】 攻撃防御システムのおとり装置において、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段を有することを特徴とするおとり装置。

【請求項 41】 攻撃防御システムのおとり装置において、

サービスプロセスの実行において、少なくともネットワーク入出力、ファイル入出力、および、プロセス生滅に係るイベントを一時的に記憶するイベント記憶手段と、

前記イベント記憶手段に記憶されたイベント間の因果関係を分析して、リンク付けを行うイベント管理手段と、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段と、

を有することを特徴とするおとり装置。

【請求項 42】 前記攻撃検知手段は、前記ドメイン制約および前記タイプ制約を判定するにあたり、前記リンクを走査して、少なくとも、検査対象であるイベントの発生源となったプロセスの生成イベントと、イベントの発生原因となったネットワーク受信イベントと、を抽出することを特徴とする請求項 41 記載のおとり装置。

【請求項 43】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、

前記ファイアウォール装置は、

入力 I P パケットに含まれる要求データおよび振り分け条件に基づいて、当該入力 I P パケットの転送先として、前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

要求データの信頼度を管理するための信頼度管理手段と、
を有し、

前記転送先選択手段は、前記入力 I P パケットに含まれる要求データに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力 I P パケットの転送先を決定することを特徴とする攻撃防御システム。

【請求項 4 4】 前記転送先選択手段は、前記信頼度管理手段から得られた入力 I P パケットに含まれる要求データに対する信頼度が、所定の閾値以上の場合に、前記内部ネットワークおよび前記おとり装置の双方に当該入力 I P パケットを転送することを特徴とする請求項 4 3 記載の攻撃防御システム。

【請求項 4 5】 前記転送先選択手段は、前記信頼度管理手段から得られた入力 I P パケットに含まれる要求データに対する信頼度が、所定の閾値よりも小さい場合に、当該入力 I P パケットを一時的に記憶する入力バッファを有し、

前記おとり装置において前記要求データが安全であることを確認した場合に、前記入力 I P パケットは前記入力バッファから前記内部ネットワークに自動的に再転送されることを特徴とする請求項 4 3 または 4 4 に記載の攻撃防御システム。

【請求項 4 6】 前記おとり装置は、請求項 3 9 ないし 4 2 のいずれかに記載のおとり装置であることを特徴とする請求項 1、7、18 および 4 3 のいずれかに記載の攻撃防御システム。

【請求項 4 7】 攻撃防御システムの攻撃検知方法において、
サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを一時的に記憶し、
イベント間の因果関係を分析してリンク付けを行う、
ことを特徴とする攻撃検知方法。

【請求項 4 8】 攻撃防御システムの攻撃検知方法において、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを抽出し、

当該イベントと、ドメイン制約またはタイプ制約を付加したルールと、を照合する、

ことを特徴とする攻撃検知方法。

【請求項 4 9】 攻撃防御システムの攻撃検知方法において、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを一時的に記憶し、

イベント間の因果関係を分析してリンク付けし、

前記イベントと、ドメイン制約またはタイプ制約を付加したルールと、を照合する、

ことを特徴とする攻撃検知方法。

【請求項 5 0】 ドメイン制約またはタイプ制約を判定するにあたり、前記リンクを走査して、少なくとも、検査対象であるイベントの発生源となったプロセスの生成イベントと、イベントの発生原因となったネットワーク受信イベントとを抽出することを特徴とする請求項 4 9 記載の攻撃検知方法。

【請求項 5 1】 内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御方法において、

I P パケットのフィルタリング条件および振り分け条件を用意し、

入力 I P パケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力 I P パケットを受理するか否かを判定し、

受理された入力 I P パケットに含まれる要求データおよび前記振り分け条件に基づいて、当該入力 I P パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力 I P パケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力 I P パケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御方法。

【請求項 5 2】 前記振り分け条件は、要求データとその信頼度との組からなる信頼度管理テーブルであり、

前記入力 I P パケットに含まれる要求データと、前記信頼度管理テーブルのあるエントリ内の要求データとが一致した場合は、当該エントリ内の信頼度を抽出し、

前記信頼度管理テーブル内に前記入力 I P パケットに含まれる要求データに一致するエントリがない場合には、当該要求データと信頼度の初期値との組である新たなエントリを作成する、

ステップを有することを特徴とする請求項 5 0 記載の攻撃防御方法。

【請求項 5 3】 前記転送先の決定において、前記信頼度管理テーブルから抽出された信頼度が、所定の閾値以上である場合に、前記内部ネットワークおよび前記おとり装置の双方を選択する、

ステップを有することを特徴とする請求項 5 1 または 5 2 に記載の攻撃防御方法。

【請求項 5 4】 前記転送先の決定において、前記信頼度管理テーブルから抽出された信頼度が、所定の閾値よりも小さい場合に、前記入力 I P パケットを一時的に記憶し、

攻撃が検知されなかった後に、当該入力 I P パケットを内部ネットワークに自動的に転送する、

ステップを有することを特徴とする請求項 5 1 または 5 2 に記載の攻撃防御方法。

【請求項 5 5】 請求項 4 7 ないし 5 0 のいずれかに記載の攻撃検知方法により前記攻撃有無の検知をすることを特徴とする請求項 1 9 または 2 7 に記載の攻撃防御方法。

【請求項 5 6】 コンピュータに、攻撃防御システムの攻撃検知を実行させるためのプログラムにおいて、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを一時的に記憶し、

イベント間の因果関係を分析してリンク付けを行う、

ステップを有することを特徴とする攻撃検知プログラム。

【請求項 57】 コンピュータに、攻撃防御システムの攻撃検知を実行させるためのプログラムにおいて、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを抽出し、

当該イベントと、ドメイン制約またはタイプ制約を付加したルールと、を照合する、

ステップを有することを特徴とする攻撃検知プログラム。

【請求項 58】 コンピュータに、攻撃防御システムの攻撃検知を実行させるためのプログラムにおいて、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを一時的に記憶し、

イベント間の因果関係を分析してリンク付けし、

前記イベントと、ドメイン制約またはタイプ制約を付加したルールと、を照合する、

ステップを有することを特徴とする攻撃検知プログラム。

【請求項 59】 内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御方法において、

IPパケットのフィルタリング条件および振り分け条件を用意し、

入力 IP パケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力 IP パケットを受理するか否かを判定し、

受理された入力 IP パケットに含まれる要求データおよび前記振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力 IP パケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力 IP パケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御プログラム。

【請求項 6 0】 前記振り分け条件は、要求データとその信頼度との組からなる信頼度管理テーブルであり、

前記入力 I P パケットに含まれる要求データと、前記信頼度管理テーブルのあるエントリ内の要求データとが一致した場合は、当該エントリ内の信頼度を抽出し、

前記信頼度管理テーブル内に前記入力 I P パケットに含まれる要求データに一致するエントリがない場合には、当該要求データと信頼度の初期値との組である新たなエントリを作成する、

ステップを有することを特徴とする請求項 5 9 記載の攻撃防御プログラム。

【請求項 6 1】 前記転送先の決定において、前記信頼度管理テーブルから抽出された信頼度が、所定の閾値以上である場合に、前記内部ネットワークおよび前記おとり装置の双方を選択する、

ステップを有することを特徴とする請求項 5 9 または 6 0 に記載の攻撃防御プログラム。

【請求項 6 2】 前記転送先の決定において、前記信頼度管理テーブルから抽出された信頼度が、所定の閾値よりも小さい場合に、前記入力 I P パケットを一時的に記憶し、

攻撃が検知されなかった後に、当該入力 I P パケットを内部ネットワークに自動的に転送する、

ステップを有することを特徴とする請求項 5 9 または 6 0 に記載の攻撃防御プログラム。

【請求項 6 3】 前記ファイアウォール装置において、

暗号化された入力 I P パケットを復号するとともに、出力 I P パケットを暗号化するための暗号処理手段を備えたことを特徴とする前記請求項 4 3 ないし 4 5 のいずれかに記載の攻撃防御システム。

【請求項 6 4】 請求項 1、7、1 8 および 4 3 のいずれかに記載の攻撃防御システムにおいて、

前記内部ネットワーク上のサーバから前記おとり装置へ少なくともファイルシステムを複製するミラーリング装置をさらに有し、

前記おとり装置で攻撃が検知されると、前記ミラーリング装置は前記内部ネットワーク上のサーバから少なくともファイルシステムを前記おとり装置へ複写することを特徴とする攻撃防御システム。

【請求項 6 5】 内部ネットワークと外部ネットワークとの境界に設置された攻撃防御システムにおいて、

おとり装置と、

ファイアウォール装置と、

前記おとり装置と前記ファイアウォール装置との間に接続されたスイッチ装置と、

を有し、

前記おとり装置は、

前記スイッチ装置から転送された入力 I P パケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有し、

前記スイッチ装置は、

前記ファイアウォール装置で受理された入力 I P パケットのヘッダ情報および振り分け条件に基づいて、当該入力 I P パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

前記攻撃検知手段が攻撃を検知した際の攻撃カテゴリと当該入力 I P パケットのアドレス情報とに対応したフィルタリング条件を生成する条件生成手段と、を有し、

前記ファイアウォール装置は、

前記条件生成手段により生成されたフィルタリング条件に従って、フィルタリング条件を動的に更新するためのフィルタリング条件制御手段と、

入力 I P パケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力 I P パケットを受理するか否かを判定するパケットフィルタリング手段と、を有する、

ことを特徴とする攻撃防御システム。

【請求項 6 6】 前記スイッチ装置は、さらに、

複数の入力 I P パケットにおける各送信元 I P アドレスの信頼度を管理するた

めの信頼度管理手段を有し、

前記転送先選択手段は、前記入力 I P パケットの送信元 I P アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力 I P パケットの転送先を決定することを特徴とする請求項 6 5 記載の攻撃防御システム。

【請求項 6 7】 前記ファイアウォール装置および前記スイッチ装置はネットワーク接続されていることを特徴とする請求項 6 5 記載の攻撃防御システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明はコンピュータネットワークにおけるセキュリティ対策に係り、特に外部ネットワークからの攻撃に対して内部ネットワーク上の資源を保護するためのシステムおよび方法に関する。

【 0 0 0 2 】

【従来の技術】

従来、外部ネットワークからの攻撃に対する防御技術として、（１）ファイアウォール、（２）侵入検知システム、（３）おとりシステム、といった手法があった。

【 0 0 0 3 】

ファイアウォールの一例は、たとえば特開平 8 - 4 4 6 4 2 号公報（特許文献 1）に開示されている。外部の I P ネットワークと内部のイーサネット（登録商標）との境界にファイアウォールを設置し、検査対象となるパケットを外部ネットワークから内部ネットワークに通過させてよいか否かを判定する。特に、ファイアウォールにパケットフィルタを設け、パケットのヘッダ情報（送信元アドレスや送信先アドレス）などの他、プロトコルの種別（T C P / U D P / H T T P など）や、データ内容（ペイロード）なども参照しながら、所定のルールに従って、パケットの通過可否を判定する。適切なルールを設定しておけば、例えば、外部ネットワーク一般に公開されている W e b サーバなどに対してワームなどを含む不正なパケットが進入することを遮断できる。

【0004】

侵入検知システムの一例は、たとえば特開 2001-350678 号公報（特許文献 2）に開示されている。この従来の侵入検知システムは不正侵入判定ルール実行部を有し、アプリケーションごとの判定ルール、例えば WWW サーバ用不正侵入判定ルールや MAIL サーバ用不正侵入判定ルールを備えている。まず、IP アドレステーブル取得部は、内部ネットワーク上を流れるパケットの送信元 IP アドレスもしくは送信先 IP アドレスから、当該 IP アドレスを持つサーバにおいて現在動作中のアプリケーションを決定する。次に、不正侵入判定ルール実行部において、そのアプリケーションに応じた不正侵入判定ルールを実行し、当該パケットが不正であるか否かを判定する。こうすることにより、アプリケーションに依存したより精度の高い侵入検知が可能となる。

【0005】

おとりシステムの第 1 例は、たとえば特開 2000-261483 号公報（特許文献 3）に開示されている。この従来のおとりシステムは、ルータ 10 の下に構築された内部ネットワーク上に、トラフィック監視装置、攻撃パターンおよび偽装サーバを備える。まず、トラフィック監視装置において、内部ネットワーク上を流れるパケットを監視しながら、特定の攻撃パターンに合致するものを不正パケットとして検出し、その識別情報（送信元 IP アドレス、送信先 IP アドレスなどを含む）をルータに通知する。次に、ルータでは、後に続く外部ネットワークからのパケットについて、検出した識別情報に合致するパケットをすべて偽装サーバに転送する。偽装サーバは、転送されたパケットを適切に解釈し、内部ネットワーク上の正規のサーバをまねた偽の応答パケットを生成し、先に不正パケットを送信したホストへ向けて、その偽の応答パケットを送信する。こうすることで、外部ネットワーク上に存在する攻撃者に、内部ネットワークに悪影響のない形で、攻撃を続けさせることができ、逆探知によって攻撃者の身元を明らかにすることができる。

【0006】

おとりシステムの第 2 例は、たとえば特開 2002-7234 号公報（特許文献 4）に開示されている。この従来のおとりシステムは、内部ネットワークと外

部ネットワーク（インターネット）との境界に、いわゆるゲートウェイとして、不正検出サーバと、おとりサーバと、を備える。外部ネットワークから内部ネットワークへ流れるパケットを不正検出サーバで監視し、例えば、当該パケットのペイロードについて所定のパターンマッチング処理を行うなどして、不正か否かを判定する。不正であると判定されたパケットには、その旨を示す特殊なマークを加えた上で、当該パケットをおとりサーバもしくは内部ネットワーク上の情報処理サーバへ転送する。情報処理サーバへ不正パケットを転送する場合、予め情報処理サーバに不正回避処理部を持たせておき、特殊なマークのあるパケットを受信した際には、さらにおとりサーバへ当該パケットを転送するようにしておく。いずれにせよ、不正検出サーバで検出された不正パケットは、最終的におとりサーバへ到達する。その後、おとりサーバでは、偽の応答パケットを生成し、不正パケットの送信元ホストに向けて、当該応答パケットを送信する。こうすることで、不正と判定されたパケットは全ておとりサーバに閉じ込めることができる。

【0007】

さらに、おとりシステムの第3例は、たとえば特開平09-224053号公報（特許文献5）に記載されている。この従来のおとりシステムは、公衆ネットワーク（インターネット）と、プライベートネットワーク（内部ネットワーク）との境界に、スクリーン・システムおよび代行ネットワークを備える。スクリーン・システムは、自身に接続される各ネットワークからの着信パケットについて、パケットのヘッダに記載される情報や着信履歴など基にしたスクリーン基準に従い、フィルタリングを行う。ただし、スクリーン・システムの通信インタフェースはIPアドレスをもたず、`traceroute`などを用いた探索から自身を隠蔽することを特徴の1つとする。もう1つの特徴として、プライベートネットワークに向かう着信パケットについて、代行ネットワークに経路を変更することもできる。代行ネットワーク上には0台以上の代行ホストが設けられ、プライベートネットワーク上にあるホストの代理として動作させることもできる。こうすることで、公衆ネットワークからの攻撃からプライベートネットワークを保護できる。

【 0 0 0 8 】**【特許文献 1】**

特開平 8 - 4 4 6 4 2 号公報（段落番号 0 0 2 9 ～ 0 0 3 0、図 5）

【特許文献 2】

特開 2 0 0 1 - 3 5 0 6 7 8 号公報（段落番号 0 0 6 2 ～ 0 0 8 4、図 1）

【特許文献 3】

特開 2 0 0 0 - 2 6 1 4 8 3 号公報（段落番号 0 0 2 4 ～ 0 0 3 0、図 1）

【特許文献 4】

特開 2 0 0 2 - 7 2 3 4 号公報（段落番号 0 0 3 6 ～ 0 0 4 0、図 1、図 2）

【特許文献 5】

特開平 0 9 - 2 2 4 0 5 3 号公報（段落番号 0 0 3 7 ～ 0 0 4 3、0 0 6 6 ～ 0 0 6 7、図 6）。

【 0 0 0 9 】**【発明が解決しようとする課題】**

しかしながら、上記従来技術は、いずれも、次に挙げるような問題点を持つ。

【 0 0 1 0 】

第 1 の問題点は、外部ネットワーク上の攻撃ホストと内部ネットワーク上のサーバとの間で、SSL（Secure Socket Layer）や IP Sec（RFC 2 4 0 1 記載）などの通信路暗号化技術が用いられた場合に、攻撃を有効に検知または防御できないということである。その理由は、攻撃検知のための主要なデータ（ペイロードなど）が暗号化されており参照できないためである。

【 0 0 1 1 】

第 2 の問題点は、攻撃検知部のパフォーマンスが、近年のネットワークの高速化に追随しきれず、検査から漏れるパケットが存在したり、ネットワークの高速性を損なったりする点にある。その理由は、攻撃検知の精度を向上するには、より多彩な、あるいはより複雑な判定ルールの実行が必要であるが、一方、ネットワークの高速化により、検査対象となるパケット量が飛躍的に増加しているため

である。

【0012】

また、特許文献2および特許文献3に記載された侵入検知システムやおとりシステムの第1例では、少なくとも1つの不正パケットが、内部ネットワーク上の保護すべきサーバに到達してしまう。その理由は、攻撃検知部が検査を行うのは、パケットのコピーでしかなく、当該パケットが不正と判定された場合でも、その内部ネットワーク上のパケット流通を遮断できないためである。

【0013】

さらに、特許文献5に記載されたおとりシステムの第3例では、インターネットから到来したパケットを代行ネットワークに経路変更させる条件および方法については検討されていない。このために、正確にパケットを振り分けることができず、正常なアクセスが代行ネットワークへ、異常なアクセスが内部ネットワークへ導かれる可能性がある。

【0014】

第3の問題点は、攻撃検知精度の向上が困難な点にある。近年のサーバ運用の形態は、遠隔からの保守作業が一般的であり、その作業はサーバ内のデータ修正やシステムの更新などであり、侵入検知システムはこうした保守作業をしばしば攻撃と誤って検知してしまう。

【0015】

また、Webアプリケーション等で知られるように、サーバのサブシステムとして、データベース操作など様々なアプリケーションプログラムを動作させることが多く、そうしたサブシステムの脆弱性を突いて不正動作を行わせる攻撃も頻繁に見られるようになった。侵入検知システムは、一般によく知られるサーバまたはそのサブシステムへの攻撃パターンを知識として備えるが、サイト独自に作成されたサブシステムが存在する場合や、一般的なサーバまたはサブシステムであっても設定に不備がある場合には、前記攻撃パターンに当てはまらない、いわゆる未知攻撃を受ける危険性がある。

【0016】

第4の問題点は、データベースやプラグインモジュールなどのサブシステムを

備えるサーバシステムにおいて、クライアントとの通信プロトコルで、一定のアクセス手順が規定されている場合（すなわちステートフルプロトコルであった場合）、不審なアクセスのみをおとりサーバなど、正規のサーバ以外に誘導する方法では、おとりサーバと正規のサーバ双方でクライアントーサーバ通信が失敗する。特に、誤っておとりサーバへ誘導されたアクセスがあった場合には、正規のサーバ上であるべき処理が行われなため、サーバ障害を発生させることになる。

【0017】

本発明の目的は、通信路暗号化技術を用いた通信システムに対しても、外部ネットワークからの攻撃を有効に防御できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

【0018】

本発明の他の目的は、高速ネットワーク環境に対応できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

【0019】

本発明のさらに他の目的は、保護すべきサーバに向けられた不正パケットを確実に遮断できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

【0020】

【課題を解決するための手段】

本発明の第1の観点によれば、おとり装置およびファイアウォール装置を含む攻撃防御システムが内部ネットワークと外部ネットワークとの境界に設置され、おとり装置はファイアウォール装置から転送された入力IPパケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有し、ファイアウォール装置は、入力IPパケットのヘッダ情報およびフィルタリング条件に基づいて当該入力IPパケットを受理するか否かを判定するパケットフィルタリング手段と、受理された入力IPパケットのヘッダ情報および振り分け条件に基づいて当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、前記おとり装置へ転送し

た入力 I P パケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて当該入力 I P パケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、を有することを特徴とする。

【0021】

本発明の第2の観点によれば、ファイアウォール装置は、入力 I P パケットのヘッダ情報および振り分け条件に基づいて当該入力 I P パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、複数の入力 I P パケットにおける各送信元 I P アドレスの信頼度を管理するための信頼度管理手段と、を有し、前記転送先選択手段は、前記入力 I P パケットの送信元 I P アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力 I P パケットの転送先を決定することを特徴とする。

【0022】

本発明による攻撃防御方法は、入力 I P パケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力 I P パケットの受理および廃棄のいずれかを実行し、受理された入力 I P パケットのヘッダ情報および振り分け条件に基づいて、当該入力 I P パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、前記入力 I P パケットが前記おとり装置へ転送されると、当該入力 I P パケットに対するサービスプロセスを実行し、前記サービスプロセスの実行状況を監視しながら、所定の攻撃カテゴリと関連づけられたルールに違反するか否かを判定することで攻撃の有無を検知し、前記入力 I P パケットに関して攻撃を検知したか否かに応じて、当該入力 I P パケットのヘッダ情報に対応するフィルタリング条件を設定し、入力した I P パケットのヘッダ情報に対応するフィルタリング条件に従ってパケットフィルタリングを実行する、ステップを有することを特徴とする。

【0023】

望ましくは、本発明によるファイアウォール装置は、入力 I P パケットのヘッダ情報およびフィルタリング条件に基づいて当該入力 I P パケットを受理するか否かを判定するパケットフィルタリング手段と、受理された入力 I P パケットの

ヘッダ情報および振り分け条件に基づいて当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を管理するための信頼度管理手段と、前記おとり装置へ転送した入力 IP パケットに関して前記おとり装置が攻撃を検知したか否かに基づいて当該入力 IP パケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、を有し、前記転送先選択手段は、前記入力 IP パケットの送信元 IP アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力 IP パケットの転送先を決定することを特徴とする。

【0024】

本発明の第3の観点によれば、おとり装置は、プロセッサから伝達される各プロセス状況について、その発生原因となった過去のプロセス状況を関連付けた上で、時系列順にメモリに格納するイベント管理手段を有することを特徴とする。さらに、プロセス状況の正常・異常を判定する際に、前記関連付けを探索して、関連プロセス状況列を分析する攻撃検知手段を有し、攻撃検知手段はプロセス状況の発生源であるプロセスと、その親プロセスとの関係、さらにアクセス元 IP アドレスとの関係などの制約の下で、当該プロセス状況の正常・異常を判定することを特徴とする。

【0025】

本発明の第4の観点によれば、ファイアウォール装置は、サーバもしくはそのサブシステムへの要求などを含むアプリケーションデータと、おとり装置における過去の攻撃検知結果とを組にして格納するハッシュ表管理部と、入力 IP パケットのペイロードを参照して、アプリケーションデータを抽出し、前記ハッシュ表管理部に当該アプリケーションデータの登録状況などを問い合わせ、その結果に応じて、前記内部ネットワークおよび前記おとり装置のいずれか、またはその双方を当該入力 IP パケットの転送先として選択する転送先選択手段と、を有し、前記転送先選択手段は、ハッシュ表管理部におけるアプリケーションデータの登録有無や、登録があった場合に攻撃として検知されているかどうかなどを確認して、登録がない場合もしくは過去に攻撃として検知されているアプリケーショ

ンデータをおとり装置へ誘導し、それ以外の場合には、内部ネットワークとおとり装置の双方へ転送することを特徴とする。

【0026】

【発明の実施の形態】

(ネットワーク構成)

図1は、本発明による攻撃防御システムの概略的ブロック図である。本発明による攻撃防御システムは、基本的に、ファイアウォール装置1およびおとり装置2を有し、インターネット3と内部ネットワーク4との境界にファイアウォール装置1が設置されている。内部ネットワーク4は、WWW (World-Wide Web) などのサービスを提供する1個以上のサーバ装置401を含む。ここではインターネット3に攻撃元ホスト301が想定されている。

【0027】

ファイアウォール装置1は、通常の正規のパケットであれば、これを通過させて内部ネットワーク4へ送付し、不正パケットあるいは不審なパケットであれば、おとり装置2へ誘導する。おとり装置2は攻撃の有無を検知し、攻撃を検知した場合にはアラートをファイアウォール装置1へ出力する。また、不正パケットに対する偽の応答パケットを生成してファイアウォール装置1へ返してもよい。ファイアウォール装置1はその偽の応答パケットを不正パケットの送信元である攻撃元ホスト301へ送信する。

【0028】

(第1実施形態)

1. 1) 構成

図2は、本発明の第1実施形態による攻撃防御システムのファイアウォール装置1およびおとり装置2の構成を示すブロック図である。ファイアウォール装置1は、外部通信インタフェース100でインターネット3と接続され、第1の内部通信インタフェース104で内部ネットワーク4と接続される。

【0029】

パケットフィルタ101は、外部通信インタフェース100および誘導部103の間に接続され、アクセス制御リスト管理部102から取得したアクセス制御

ルールに従ってパケットフィルタリングを行う。後述するように、外部通信インタフェース 100 または誘導部 103 の一方から受け取った IP パケットを他方へ転送し、あるいは転送せずに廃棄する。

【0030】

パケットフィルタ 101 で受理されたパケットは誘導部 103 へ送られ、誘導部 103 は、後述する誘導リスト (図 5) を参照し、パケットフィルタ 101 から入力した IP パケットの宛先 IP アドレスに応じて当該パケットを第 1 の内部通信インタフェース 104 および第 2 の内部通信インタフェース 105 のいずれかへ誘導する。逆に、第 1 の内部通信インタフェース 104 または第 2 の内部通信インタフェース 105 からインターネット 3 に向かう IP パケットをパケットフィルタ 101 に転送する。

【0031】

第 1 の内部通信インタフェース 104 は、誘導部 103 から入力した IP パケットを内部ネットワーク 4 に伝達し、内部ネットワーク 4 からインターネット 3 に向かう IP パケットを誘導部 103 へ伝達する。第 2 の内部通信インタフェース 105 は、誘導部 103 によって誘導された IP パケットをおとり装置 2 に伝達し、おとり装置 2 からインターネット 3 に向かう IP パケットを誘導部 103 に伝達する。

【0032】

おとり装置 2 は、プロセッサ 201 と攻撃検知部 202 とを含む。プロセッサ 201 は、WWW や Telnet などのネットワークサービスを提供するプロセスを実行しながら、当該プロセスの状況を攻撃検知部 202 へ随時伝達する。攻撃検知部 202 は、プロセッサ 201 から入力されるプロセス状況を監視しながら、攻撃の有無を検査し、攻撃が認められた場合には攻撃内容を報告するためのアラートを生成しファイアウォール装置 1 へ送出する。

【0033】

制御インタフェース 106 を通してアラートを入力すると、防御ルール判定部 107 は、アラートの内容に従ってアクセス制御リスト管理部 102 のアクセス制御リストの更新等を指示する。

【0034】

図3は、図2のファイアウォール装置1におけるアクセス制御リスト管理部102の模式的構成図である。アクセス制御リスト管理部102は、アクセス制御リストデータベース1021、検索部1022および更新処理部1023を有する。アクセス制御リストデータベース1021は、少なくとも「ソースIPアドレス」、「ディスティネーションIPアドレス」および「フィルタ処理方法」といったフィールドを有するエントリ（アドレス制御ルール）の集合を検索可能に保持する。検索部1022は、パケットフィルタ101からIPアドレスなどを含む問い合わせ（RQ）を受けると、アクセス制御リストデータベース1021から対応するアクセス制御ルールを検索してパケットフィルタ101へ返す。更新処理部1023は、防御ルール判定部107から入力した更新用アクセス制御ルールに従ってアクセス制御リストデータベース1021の内容を更新（追加／修正）する。

【0035】

図4は、アクセス制御リストデータベース1021の内容を例示した模式図である。アクセス制御リストデータベース1021には複数のアクセス制御ルールが所定の規則に従って格納される。各アクセス制御ルールは、図4に示すように、ソースIPアドレス（SRC）やディスティネーションIPアドレス（DST）などのルール適合条件と、パケットの受理（ACCEPT）、拒否（DENY）、廃棄（DROP）などの所定の処理方法（PROC）を示す識別子との組からなる。アクセス制御ルールは一般に複数設定されるので、その集合をアクセス制御リストデータベース1021で保持しておく。図4において、アスタリスク（*）は任意のアドレスを示し、パケットフィルタ処理の“ACCEPT”はパケットの受理、“DENY”はICMPエラー通知をするパケット拒否、“DROP”はICMPエラー通知をしないパケット廃棄をそれぞれ示す。

【0036】

図5は、誘導部103に設けられた誘導リストの一例を示す模式図である。誘導部103には、予め1つ以上のIPアドレスからなる誘導リストが保持されている。本実施例の誘導リストでは、内部ネットワーク4の未使用IPアドレスが

列挙されている。後述するように、未使用であるはずの IP アドレスを宛先とするパケットは、不審パケットである可能性が高い。

【0037】

図6は、防御ルール判定部107に保持されている防御ルールスクリプトを例示した模式図である。詳しくは後述するが、防御ルール判定部107は、探査 (RECON)、侵入 (INTRUSION)、破壊 (DESTRUCTION) などの攻撃種別ごとに、防御ルールを列挙し、例えばファイル形式で保持している。防御ルールは、所定の攻撃カテゴリに1対1対応する形式で、1つのアクセス制御ルールの雛型を指定する記述が用いられる。例えば、

```
INTRUSION: (SRC: $ {SOURCE_IP_ADDRESS}  
, DST: *, PROC: DROP)
```

といった記述が行ごとに攻撃種別ごとに列挙されている。この記述のうち「\$ {SOURCE_IP_ADDRESS}」の部分が、後述するように、おとり装置2からのアラートに記載された情報 (攻撃パケットのソース IP アドレス) で置き換えられる変数である。

【0038】

1. 2) 動作

1. 2. 1) パケットフィルタリング

図7は、本発明の第1実施形態による攻撃防御システムの動作を示すフローチャートである。まず、ファイアウォール装置1において、インターネット3から内部ネットワーク4へ向けた IP パケットを外部通信インタフェース100で捉えた後、当該 IP パケットをパケットフィルタ101へ転送する (ステップA1)。

【0039】

次に、パケットフィルタ101は、当該 IP パケットのヘッダを参照し、そこに記載されているソース IP アドレスやディスティネーション IP アドレスなどの情報をアクセス制御リスト管理部102へ出力する。アクセス制御リスト管理部102は、上述したように、入力した IP アドレスを用いてアクセス制御リストデータベース1021を検索し、ヒットした最初のアクセス制御ルールをパケ

ットフィルタ 101 へ返す。アクセス制御ルールを取得すると、パケットフィルタ 101 は、その処理方法に従って、当該 IP パケットを受理または廃棄する（ステップ A2）。IP パケットを受理した場合は、当該 IP パケットを誘導部 103 へ転送し、廃棄した場合は、直ちに次のパケットの処理へと制御を移す。

【0040】

アクセス制御リスト管理部 102 におけるアクセス制御ルールの検索において、パケットフィルタ 101 から入力したソース IP アドレスを検索部 1022 が受け取ると、検索部 1022 は個々のアクセス制御ルールの適合条件と入力したソース IP アドレスとを照合し、適合条件を満たす最初のアクセス制御ルールを抽出し、パケットフィルタ 101 へ返す。

【0041】

1. 2. 2) パケット誘導

次に、誘導部 103 では、パケットフィルタ 101 で受理された IP パケットに対して、そのディスティネーション IP アドレスと予め設けられた誘導リストとを参照し、転送すべき内部通信インタフェース（104 あるいは 105）を決定する（ステップ A3）。具体的には、図 5 に示すような誘導リストと、ディスティネーション IP アドレスとを照合し、合致するものがある場合には、第 2 の内部通信インタフェース 105 を介して当該 IP パケットをおとり装置 2 へ転送する。合致するものがない場合には、第 1 の内部通信インタフェース 104 を介して内部ネットワーク 4 へ当該 IP パケットを伝達する。

【0042】

IP パケットが内部ネットワーク 4 へ伝達された場合には、当該 IP パケットは内部ネットワーク 4 上の適切なサーバ装置 301 に到達し、所定のサービスを提供するための処理が行われる（ステップ A4）。

【0043】

一方、IP パケットがおとり装置 2 へ伝達された場合には、そのプロセッサ 201 において、偽のサービスを提供するための処理を行いながら、入力データの内容や処理状況を逐次的に攻撃検知部 202 へ通知する（ステップ A5）。この際、おとり装置 2 は、ファイアウォール装置 1 から伝達された IP パケットを、

そのディスティネーション IP アドレスの如何を問わず、受信することができる。具体的には、おとり装置 2 に複数の IP アドレスを割り当てられるような工夫を施してもよいし、あるいは図 8 に示すように、予め誘導部 103 にアドレス変換部 1031 を備えておき、入力 IP パケットのディスティネーション IP アドレスをおとり装置 2 の IP アドレスに書き換えた上で、おとり装置 2 に当該 IP パケットを伝達するような方法を用いてもよい。

【0044】

1. 2. 3) 偽サービス提供

IP パケットを受信後、おとり装置 2 は、偽のサービスとして、WWW や T e l n e t など 1 つ以上の任意のものを提供する。ただし、本実施形態においては、通信プロトコルさえ適切に処理すれば十分であり、実際のサービスで行われるような、ファイルシステムへのアクセスやデータベース処理などは一切行わなくともよい。具体的には、例えば、T e l n e t サービスの場合であれば、L o g i n / P a s s w o r d プロンプトへの任意の入力に対して、すべてログインを許可し、ユーザに偽のメッセージを応答するような偽装シェルを起動するようにしてもよい。

【0045】

1. 2. 4) 攻撃検知

次に、おとり装置 2 の攻撃検知部 202 では、プロセッサ 201 から通知される処理状況について、正常動作定義との照合を行い、攻撃の有無を判定する（ステップ A6）。正常動作定義とは、おとり装置 2 上で提供されるサービスの正しい振舞いに関する条件の集合である。具体的には、例えば、WWW サービスに対して「WWW サービスに対応するプロセスは自ら他のサーバ装置にネットワークアクセスをすることはない」というような条件や、「/ u s r / l o c a l / w w w / l o g s ディレクトリ以外にファイルを書き込むことはない」というような条件などの集合である（詳しくは、図 12 参照）。これらの各条件と通知された処理状況とを照合し、合致しない条件を少なくとも 1 つ検出した際に、「攻撃あり」と判断する。

【0046】

攻撃を検出した際、違反した条件の意味に応じて、攻撃種別を決定し、その結果をアラートとしてファイアウォール装置 1 へ送信する（ステップ A 7）。

【0047】

攻撃種別とは、当該攻撃に対する防御方法を導出するのに十分な分類をいい、例えば、

- ・「探査」：ポートスキャンやバナー攻撃などのいわゆる「フィンガープリンティング」

- ・「侵入」：トロイの木馬やアカウントの追加などのバックドア設置

- ・「破壊」：Ping Of Deathなどのサービス不能攻撃

などを指す。その方法の一例として、正常動作定義の中の各条件について、違反時に想定される攻撃種別を予め併記しておけばよい。例えば、前記した「/usr/local/www/logs ディレクトリ以外にファイルを書き込むことはない」という条件に違反するような攻撃については、バックドア設置の可能性が高いので、「侵入」を示す識別子を当該条件に併記しておく。

【0048】

1. 2. 5) アクセス制御リストの更新

最後に、ファイアウォール装置 1 における防御ルール判定部 107 では、制御インタフェース 106 を介しておとり装置 2 から受信したアラートを参照し、防御ルールを用いてアクセス制御ルールを生成し、アクセス制御リスト管理部 102 へ当該アクセス制御ルールを追加するよう指示する（ステップ A 8）。

【0049】

具体的には、防御ルール判定部 107 に、予め攻撃種別ごとに、図 6 のような防御ルールスクリプトを設定しておく。防御ルールスクリプトには、図 6 のような書式によって、攻撃種別と更新すべきアクセス制御ルールのひな型との組を記述する。アクセス制御ルールのひな型には、アラートに記載された情報を挿入するための変数が記述できる。たとえば、

(SRC:\$ {SOURCE__IP__ADDRESS}, DST:1. 2. 3. 4, PROC:DROP)

と記述されている場合、「\$ {SOURCE__IP__ADDRESS}」の箇所

は、アラートに記載されたソース IP アドレスで置換され、

(SRC: 12. 34. 56. 78, DST: 1. 2. 3. 4, PROC: DROP)

といった完全な形式のアクセス制御ルールに変換される。そして、当該アクセス制御ルールは、アクセス制御リスト管理部 102 内の更新処理部 1023 へ伝達され、アクセス制御リストデータベース 1021 に適切に追加される。同じソース IP アドレスおよびディスティネーション IP アドレスの組をもつアクセス制御ルールが既にアクセス制御リストデータベース 1021 に登録されている場合には、更新処理部 1023 は、新たに追加されたアクセス制御ルールが有効になるように適切にアクセス制御リストデータベース 1021 を更新する。たとえば、アクセス制御リストデータベース 1021 の検索スキャン方向の先頭に位置するように追加される。

【0050】

1. 3) 効果

第 1 実施形態のファイアウォール装置 1 では、誘導部 103 において、誘導リストとディスティネーション IP アドレスとの照合結果により、おとり装置 2 へ誘導する方法を用いている。このために、内部ネットワーク 4 の既存の構成を一切変更することなく、おとり装置 2 を設置可能となる。さらに、誘導リストに含める IP アドレスとして、内部ネットワーク 4 における未使用の IP アドレス群を記載することで、1 台のおとり装置 2 で、内部ネットワーク 4 上に複数のおとり装置 2 を設置するのと同じ効果が得られる。

【0051】

通常、「Code Red」や「Nimda」などの自動感染機能をもつワームは、ある連続した IP アドレスの区間からランダムに IP アドレスを選択しながら、感染を試みるよう動作する。したがって、おとり装置 2 は設置台数が多ければ多いほど検知の確率が高くなる。本実施形態では、図 5 に示すような誘導リストの作成でその効果を得ることができる。

【0052】

また、ファイアウォール装置 1 の外部通信インタフェース 100 に割り当てら

れたIPアドレスを誘導リストに含めることで、インターネット3側からは、ファイアウォール装置1とおとり装置2との見分けがつかなくなる。一般に、インターネット3からの攻撃は、ファイアウォールの発見から始まるので、本実施形態はファイアウォール装置1を「隠す」という効果をもつ。

【0053】

1. 4) 具体例

図9～図11は第1実施形態の具体的動作例を説明するためのネットワーク構成図であり、図12はおとり装置2における攻撃検知動作を説明するための模式図である。

【0054】

図9に示すように、インターネット3上に攻撃元ホスト301（IPアドレス：12.34.56.78）があり、内部ネットワーク4上にインターネットサーバ装置401がありものとする。さらに、インターネット3と内部ネットワーク4との境界にファイアウォール装置1が設置され、標準的なポート番号であるTCP80番ポートにおいてWWWサービスを提供するおとり装置2が設置されているものとする。また、内部ネットワーク4のネットワークアドレスとして、「1.2.3.x/24」が用いられており、サーバ装置401には「1.2.3.4」というIPアドレスが設定されているものとする。

【0055】

今、攻撃元ホスト301はWWWサービスに対する自動感染機能をもつワームに感染しており、当該ワームが次の感染先として、内部ネットワーク4に対応する「1.2.3.x/24」に狙いを定め、かつ「1.2.3.1」を第1の感染先として選択したものとする。このとき、攻撃元ホスト301から内部ネットワーク4に向けて、SYNパケット（ソースIPアドレス：12.34.56.78、デスティネーションIPアドレス：1.2.3.1）が送信される。

【0056】

当該SYNパケットは、まず、ファイアウォール装置1の外部通信インタフェース100に到達した後、ただちにパケットフィルタ101に伝達される。パケットフィルタ101では、アクセス制御リスト管理部102に対して、少なくと

も当該SYNパケットのソースIPアドレス「12.34.56.78」とディスティネーションIPアドレス「1.2.3.1」とを出力する。この他、アクセス制御ルールの粒度を高めるために、プロトコル番号「6」（TCPを示す）や、ポート番号「80」などを出力できるようにしてもよいが、本実施例では例としてソースIPアドレスとディスティネーションIPアドレスだけを入力するものとする。

【0057】

アクセス制御リスト管理部102におけるアクセス制御リストデータベース1021は、例えば、図4のようなテキスト形式で記述されたアクセス制御リストを保持しているものとする。上述したように、各行は1つのアクセス制御ルールを示しており、SRCフィールドとDSTフィールドとの組が適合条件を、PROCフィールドがフィルタ処理方法をそれぞれ示す。

【0058】

検索部1022では、パケットフィルタ101から入力として与えられたソースIPアドレス「12.34.56.78」およびディスティネーションIPアドレス「1.2.3.1」との組を検索キーとして、適切なアクセス制御ルールを抽出するために、アクセス制御リストデータベースの先頭行から順に各アクセス制御ルールを参照しながら、各ルールの適合条件と前記入力との比較を行い、適合する最初のアクセス制御ルールを抽出する。この時点では、「(SRC:*, DST:1.2.3.1, PROC:ACCEPT)」(「PROC:ACCEPT」は入力IPパケットの受理を示す)というアクセス制御ルールが適合したとする。このとき、検索部1022は、「(SRC:12.34.56.78, DST:1.2.3.1, PROC:ACCEPT)」をパケットフィルタ101に返す。

【0059】

アクセス制御ルールを受け取ったパケットフィルタ101は、当該ルールのPROCフィールドを参照し、「ACCEPT」であることを確認すると、ただちに入力IPパケットを後段の誘導部103へと伝達する。

【0060】

【 0 0 6 1 】

【 0 0 6 2 】

【 0 0 6 3 】

出証特 2 0 0 3 - 3 0 6 8 0 3 4

ク上のシステム領域にコピーした後、当該コードを実行するようなコマンドを発行する。したがって、ワームの侵入時に、プロセッサ 201 は、システム領域へファイルの書き出しが行われたこと、あるいは、当該ファイルの実行が行われたことを攻撃検知部 202 に伝達することになる。このとき、同時に、おとり装置 2 が受け付けた入力 IP パケットのコピーも併せて伝達する。

【0064】

攻撃検知部 202 は、予めプロセッサ 201 上の WWW サービスの適正な動作に関する情報を、正常動作定義ファイルとして保持している。正常動作定義ファイルは、例えば、図 12 のような形式で記述されており、ファイルの読み込み、書き出し、実行などに関する条件が列挙されている。

【0065】

ここで、前記ワームが自身のコピーを書き出す箇所を「C:¥Windows」ディレクトリだとすると、その動作は図 12 に示す正常動作定義ファイル内の第 2 番目の条件である

「WRITE, C:¥Inetpub¥wwwroot¥__vti__log¥* ; INTRUSION」(「C:¥Inetpub¥wwwroot¥__vti__log ディレクトリ以下にのみファイル書き出しを行う」の意)

に違反する。このとき、攻撃検知部 202 は、当該条件の「;」以下を参照し、INTRUSION (侵入) カテゴリに属する攻撃があったと判定する。

【0066】

続いて、攻撃検知部 202 は、少なくとも、入力 IP パケットに含まれるソース IP アドレスと、検出された攻撃のカテゴリが「INTRUSION」であることを知らせるためのアラートを生成し、ファイアウォール装置 1 の制御インタフェース 106 へ伝達する(図 11 参照)。

【0067】

制御インタフェース 106 で受信されたアラートは防御ルール判定部 107 へ伝達される。アラートの入力を受けた防御ルール判定部 107 は、上述したように、防御ルールを列挙したスクリプトを、例えばファイル形式で保持している。各防御ルールは、所定の各攻撃カテゴリに 1 対 1 対応する形式で、1 つのアクセ

ス制御ルールのかな型が指定されている(図6参照)。

【0068】

具体的には、例えば、

```
INTRUSION: (SRC:$ {SOURCE_IP_ADDRESS}  
, DST:*, PROC:DROP) . . . (1)
```

といった記述が行ごとに列挙されている。ここで、アラートの入力を受けた防御ルール判定部107は、防御ルールの定義ファイルを行ごとに参照し、「INTRUSION」カテゴリに対応する防御ルールである式(1)を抽出する。そして、アクセス制御ルールの雛型に対して、当該アラートに記載されたソースIPアドレス「12.34.56.78」(すなわち攻撃元ホストのIPアドレス)によって、「\$ {SOURCE_IP_ADDRESS}」を置換し、

```
(SRC:12.34.56.78, DST:*, PROC:DROP)  
. . . (2)
```

というアクセス制御ルールを生成する(「DST:＊」は任意のディスティネーションIPアドレスに適合する)。そして、当該アクセス制御ルールをアクセス制御リスト管理部102へ伝達する。

【0069】

アクセス制御リスト管理部102では、防御ルール判定部107からのアクセス制御ルールの入力について更新処理部1023で処理する。更新処理部1023では、式(2)で示されるアクセス制御ルールを、アクセス制御リストデータベース1021に伝達し、その追加を指示する。アクセス制御リストデータベース1021では、式(2)で示されるアクセス制御ルールを追加するように更新処理を行う。その際、アクセス制御リストデータベース1021は、それ以降の検索処理が最近の更新結果を反映するように適切に更新処理を行う。例えば、図4のようなテキスト形式で記述されたアクセス制御リストを用い、先頭行から順に検索処理を行うような場合であれば、式(2)を先頭行に追加すればよい。つまり、たとえ次式(3)といったようなアクセス制御ルールが予め設定されていたとしても、

```
(SRC:12.34.56.78, DST:*, PROC:ACCEPT)
```

．．．（３）

当該更新処理以降、検索部 1 0 2 2 がソース IP アドレス「1 2 . 3 4 . 5 6 . 7 8」を含む入力を受けた場合には、式（３）ではなく式（２）を検索結果として出力する（図 1 3 参照）。

【 0 0 7 0 】

次に、攻撃元ホスト 3 0 1 上のワームが次の攻撃先として、「1 . 2 . 3 . 4」を選択したものとする。しかる後、先の攻撃と同様に、内部ネットワーク 4 上のサーバ装置 4 0 1 に向けた SYN パケットがファイアウォール装置 1 に到達する。その場合、当該 SYN パケットの入力をうけたパケットフィルタ 1 0 1 は、アクセス制御リスト管理部 1 0 2 から適合するアクセス制御ルールとして式（２）を受け取るので、PROC フィールドの指定「DROP」に従い、当該 SYN パケットを廃棄する（図 1 4 参照）。

【 0 0 7 1 】

以上のような動作を行うことにより、本発明による攻撃防御システムは、攻撃元ホスト 3 0 1 上のワームからの攻撃から、内部ネットワーク 4 上のサーバ装置 4 0 1 を保護することができる。

【 0 0 7 2 】

（第 2 実施形態）

2 . 1）構成

図 1 5 は、本発明の第 2 実施形態による攻撃防御システムのブロック図である。本実施形態のファイアウォール装置 5 は、図 2 に示す第 1 実施形態におけるファイアウォール装置 1 に信頼度管理部 5 0 2 を加え、さらに誘導部 1 0 3 に代えて、信頼度に依存してパケット誘導方向を決定できる誘導部 5 0 1 を有する。以下、図 2 に示すシステムと同じ機能ブロックについては、同一参照番号を付して詳細な説明は省略する。

【 0 0 7 3 】

図 1 5 において、誘導部 5 0 1 は、パケットを入力すると、信頼度管理部 5 0 2 へ入力 IP パケットのソース IP アドレスを出力し、対応する信頼度を取得する。信頼度を受け取ると、誘導部 5 0 1 はその信頼度と所定のしきい値との比較

を行い、その結果に応じて、当該入力 IP パケットを第1の内部通信インタフェース 104 および第2の内部通信インタフェース 105 のいずれかに出力する。

【0074】

信頼度管理部 502 は IP アドレスと対応する信頼度との組の集合を管理する。誘導部 501 から要求があると、信頼度管理部 502 はそれに対応した信頼度を検索して誘導部 501 へ返し、後述するように信頼度の更新を行う。

【0075】

2. 2) 動作

図 16 は、本発明の第2実施形態による攻撃防御システムの動作を示すフローチャートである。

【0076】

まず、第1実施形態のファイアウォール装置 1 と同様に、インターネット 3 からの入力 IP パケットを受信すると（ステップ A1）、パケットフィルタ 101 は、アクセス制御リスト管理部 102 で保持されているアクセス制御ルールの内容に応じて、当該入力 IP パケットの受理または廃棄を行う（ステップ A2）。受理された IP パケットは誘導部 501 へ転送される。

【0077】

2. 2. 1) 信頼度管理

誘導部 501 は、入力 IP パケットに含まれる情報のうち少なくともソース IP アドレスを信頼度管理部 502 へ出力し、当該 IP アドレスに対する信頼度を取得する（ステップ C1）。信頼度管理部 502 は IP アドレスとその信頼度との組の集合を保持し、IP アドレスを入力すると、それに対応する信頼度を出力することができる。具体的には、例えば、「1. 2. 3. 4 : 10」などのように、「<IP アドレス> : <信頼度>」といった形式をなす行で構成されるテキストファイルを用いることができる。

【0078】

その他、検索および更新処理を効率的に行うために、リレーショナルデータベースを利用してもよい。いずれにせよ、任意の IP アドレスについて、対応する信頼度を適切に検索および更新できればよい。信頼度管理部 502 は、入力され

た IP アドレスに対応する IP アドレスと信頼度との組が 1 つ見つければ、当該信頼度を誘導部 501 へ出力する。もし適切な IP アドレスと信頼度の組が見つからなかった場合には、当該 IP アドレスに対する信頼度として初期値（例えば 0）を設定し、当該初期値を誘導部 501 に出力するとともに、新たに「< IP アドレス>：< 初期値>」という組を保持内容に追加する。

【0079】

続いて、信頼度管理部 502 は、信頼度を出力した後、当該信頼度を増加させるように保持内容を更新する（ステップ C2）。具体的には、例えば次式（4）に示されるように、信頼度に定数 C（ ≥ 1 ）を加算する。

$$c[n+1] = c[n] + C \quad \cdots \quad (4)。$$

【0080】

2. 2. 2) 信頼度に基づくパケット誘導

誘導部 501 は、取得した信頼度に応じて、当該 IP パケットの転送先を決定する（ステップ C3）。信頼度 c の評価処理の好適な一例としては、予め誘導部 501 にあるしきい値 T を設定しておき、信頼度 c としきい値 T との比較結果（大小関係）を評価する。

【0081】

図 17 は、本実施形態における信頼度とパケット転送先の関係を示すグラフである。ここでは、 $c \geq T$ のときには、入力 IP パケットを「信頼できる」と判定し、当該 IP パケットを内部通信インタフェース 104 を介して内部ネットワーク 4 へ伝達する。一方、 $c < T$ のときには、内部通信インタフェース 105 を介して、おとり装置 2 へ伝達する。

【0082】

なお、これ以降の動作は、図 7 に示す処理（ステップ A4～A8）と同じである。

【0083】

2. 2. 3) 信頼度の更新方法

図 16 のステップ C2 における信頼度の更新方法は、上述した式（4）の他に、別の方法もある。次式（5）に示すように、誘導部 501 からの入力の一部に

、入力 IP パケット p のバイト数 $L(p)$ を含めておき、その逆数 $1/L(p)$ を加算するようにしても良い。

$$c[n+1] = c[n] + 1/L(p) \quad \dots \quad (5)。$$

【0084】

この方法は、大きなサイズをもつ IP パケットほど信頼度が増加しにくくなるように、重みづけを行うものである。一般に、バッファオーバーフロー攻撃やサービス妨害 (DoS) 攻撃を目的とした IP パケットは正常な通信内容をもつ IP パケットに比べて大きなサイズをもつことが多いため、こうした重みづけを施すことで、これらの攻撃の可能性をもつ入力 IP パケットを、できるだけ長い期間、おとり装置 2 へ誘導することが可能になる。その結果、本発明による攻撃防御システムの防御性能を高めることができる。

【0085】

また、別の一例として、誘導部 501 からの入力の一部に、入力 IP パケットのプロトコル番号を含めておき、予め設定されたプロトコル番号に一致した場合のみ、信頼度を更新する方法を併用してもよい。たとえば、予めプロトコル番号「6」を設定しておくことで、入力 IP パケットが TCP である場合にのみ、信頼度を更新する。こうすることで、本格的な攻撃の前に準備的に行われるスキャン攻撃による、不要な信頼度の増加を抑える効果が得られる。もちろん、更新処理の条件として、プロトコル番号だけでなく、その他 IP ヘッダ、TCP ヘッダ、UDP ヘッダなどに含まれる任意の情報を用いてもよいし、複数の条件を組み合わせた論理式を用いるようにしてもよい。

【0086】

さらに別の一例として、入力 IP パケットについて、一般に外れ値検知として知られるような、統計的に「異常であること」の確からしさを求める方法を用いてもよい。具体的には、図 18 に示すように、IP アドレスと信頼度との組の集合に代えて、特開 2001-101154 公報 (本出願人による特許出願) に記載の外れ値度計算装置を信頼度管理部 502 に組み込む。この場合、誘導部 501 からは実数値や属性を表す離散値などを含む多次元のベクトル、たとえば、 $x = (\text{入力 IP パケットの到達時刻、入力 IP パケットのサイズ、プロトコル番号}$

)を入力する。

【0087】

このような多次元ベクトルを入力した外れ値度計算装置は、それまでの入力から生成した確率密度分布などを基に、1個の実数値として表される「スコア値」を算出する。このスコア値は「異常であること」の確からしさを表しており、その値が大きいほど攻撃である可能性が高い、言い換えれば信頼度が低い。したがって、スコア値の逆数でもって、入力IPパケットに対する信頼度とすることができる。

【0088】

図18(A)は、外れ値度計算を用いた信頼度管理部502の概略的構成図であり、(B)は、その一例を示す詳細なブロック図である。この外れ値度計算を用いる方法は、上述したような「決定的な」信頼度の評価方法では捉えきれない(すなわち予期されない)攻撃を「確率的に」検出するものである。したがって、将来現れうる未知の攻撃に対する防御が可能となる。

【0089】

本発明の第2実施形態は、第1実施形態による効果に加えて、さらに「アクティブ・ターゲッティング」にも対応できるという効果が得られる。アクティブ・ターゲッティングとは、次に具体的に説明するように、予め特定のサーバ装置もしくはホスト装置に狙いを定めて行われる攻撃形態を指し、一般的には悪意をもった人間によって実行される。

【0090】

2.3) 具体例

図19～図21は、本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【0091】

図19に示すように、インターネット3上の攻撃元ホスト301を使うユーザが、内部ネットワーク4上のサーバ装置401の動作停止を目的として、Ping Of DeathなどのDoS攻撃を行う場合を考える。

【0092】

このような場合、攻撃元ホスト 301 の IP アドレス「12.34.56.78」に対する信頼度が、誘導部 501 に設定されたしきい値以下であれば、図 20 に示すように、D o S 攻撃を構成する IP パケットはおとり装置 2 へ誘導され、サーバ装置 401 は保護される。D o S 攻撃をしかけるような悪意をもった人間は、ターゲットを定めたしばらく後に、攻撃を開始すると考えられるので、前記しきい値を十分大きく設定しておくことで、おとり装置 2 によるサーバ装置 401 の保護が達成される。

【0093】

さらに、通常の（すなわち攻撃の意図がない）ユーザからのアクセスについては、安全に内部ネットワーク 4 上のサーバ装置 401 によるサービスを行うができる。たとえば、図 21 に示すように、インターネット 3 上に通常のホスト 302 から、サーバ装置 401 へのアクセスがあった場合、前記例と同様に、ファイアウォール装置 5 の信頼度管理部 502 により、通常のホスト 302 の IP アドレスに対する信頼度が評価される。

【0094】

もし、通常のホスト 302 の信頼度が不十分であれば、誘導部 501 により「不審」と判定され、おとり装置 2 へ当該アクセスを構成する IP パケットは誘導される。ここで、おとり装置 2 のプロセッサ 201 で、サーバ装置 401 上の WWW サービスと同じ処理を行うよう、おとり装置 2 を設定しておく。すなわち、おとり装置 2 をサーバ装置 401 のミラーサーバとして動作させる。具体的には、WWW サービスの場合、HTML ファイルや JPEG ファイルなどのコンテンツの複製をとればよい。したがって、通常のホスト 302 は目的のサービスを受けることができる。おとり装置 2 では正常なアクセスがなされる間は攻撃が検知されないことがないので、通常のホスト 302 の IP アドレスに対する信頼度は上述した信頼度更新方法に従って増加していき、いずれ、しきい値 T を超える。信頼度 c がしきい値 T を超えた後は、通常のホスト 302 からのアクセスを構成する IP パケットは内部ネットワーク 4 内のサーバ装置 401 へ誘導される。

【0095】

このような動作により、信頼ずみの通常のユーザからのアクセスについては、

すべてサーバ装置 401 が応答する。したがって、おとり装置 2 が攻撃を受けて、その動作を停止したとしても、信頼ずみの通常のユーザは、サーバ装置 401 によりサービスを継続して受けることができるという効果をもつ。

【0096】

なお、おとり装置 2 はサーバ装置 401 上の完全なミラーサーバとして設定してもよいし、例えば、ユーザ認証を要するような重要サービスは除いて、一般的なサービスだけをおとり装置 2 で提供するようにも設定できる。

【0097】

(第3実施形態)

図 22 は、本発明の第3実施形態による攻撃防御システムのファイアウォール装置の概略的構成を示すブロック図であり、図 23 は、その一例を示す詳細なブロック図である。本実施形態のファイアウォール装置 6 は、ファイアウォール装置 1 における誘導部 103 に加えて、図 5 に示す第2実施形態の誘導部 501 および信頼度管理部 502 を有する。

【0098】

具体的には、図 23 に示すように、第1の誘導部 103 の後段として第2の誘導部 501 を設けても良い。逆に、第1の誘導部 103 の前段として第2の誘導部 501 を設けることもできる。

【0099】

いずれの構成においても、ワームのようにランダムに IP アドレスを選択して行われる攻撃と、アクティブ・ターゲッティングによる攻撃の両方に対応できる、という効果が得られる。また、あるホストが、第2の誘導部 501 で一旦信頼された後、ワームに感染するなどした場合でも、おとり装置 2 にて攻撃の有無を検査することができる、という効果も得られる。

【0100】

(第4実施形態)

4. 1) 構成

図 24 は、本発明における第4実施形態による攻撃防御システムのファイアウォール装置の一例を示すブロック図である。本実施形態によるファイアウォール装

置 7 は、図 15 のファイアウォール装置 5 における信頼度管理部 502 に代えて、信頼度管理部 701 が接続されている。その他の機能ブロックは、図 15 のものと同じであるから、同一参照番号を付して説明は省略する。

【0101】

図 24 に示すように、信頼度管理部 701 は、リアルタイム信頼度データベース 7011、複製処理部 7012、長期信頼度データベース 7013、および、更新処理部 7014 を備える。

【0102】

リアルタイム信頼度データベース 7011 は、IP アドレス、それに対応する信頼度および最終更新時刻の組の集合を管理し、誘導部 501 からの問い合わせの IP アドレスに応じて、対応する信頼度を返す。複製処理部 7012 は、定期的に、リアルタイム信頼度データベース 7011 の内容を、長期信頼度データベース 7013 へ複製する。

【0103】

長期信頼度データベース 7013 は、IP アドレス、それに対応する信頼度および最終更新時刻の組の集合を管理する。更新処理部 7014 は、定期的に長期信頼度データベース 7013 を参照し、所定の期間よりも古い最終更新時刻を有する項目について、その信頼度を減算する更新処理を実行する。

【0104】

4. 2) 信頼度管理

基本的には、入力 IP パケットをフィルタリングし、おとり装置 2 または内部ネットワーク 3 へ誘導するまでの処理は、第 2 実施形態のファイアウォール装置 5 と同一である（図 16 のステップ A1～A2、C1～C3、A4～A8）。ただし、本実施形態の信頼度管理部 701 は、パケットの処理と並行して、以下にあげるような信頼度管理処理を行う。

【0105】

図 25 は信頼度管理部 701 における信頼度参照処理を示すフローチャートである。まず、図 16 のステップ C1 において信頼度の参照が行われたとき、信頼度管理部 701 は、リアルタイム信頼度データベース 7011 から、入力として

特願2003-074781

与えられたIPアドレスに対応する項目が記録されているかどうかを調べる(図25のステップD1)。当該IPアドレスに対応する項目が記録されている場合(ステップD1のY)、さらにその信頼度を参照し、当該信頼度を誘導部501に出力する(ステップD2)。

【0106】

一方、IPアドレスに対応する項目がリアルタイム信頼度データベース7011に記録されていない場合(ステップD1のN)、まず、長期信頼度データベース7013を参照して、当該IPアドレスに対応する項目が記録されているかどうかを調べる(ステップD3)。記録されている場合(ステップD3のY)、長期信頼度データベース7013の該当項目の内容(IPアドレス、信頼度および最終更新時刻)を、リアルタイム信頼度データベース7011にコピーし(ステップD4)、信頼度を出力する(ステップD2)。長期信頼度データベース7013にも該当項目がない場合(ステップD3のN)、リアルタイム信頼度データベース7011に、所定の信頼度の初期値をもって、新たな項目を追加し(ステップD5)、信頼度を出力する(ステップD2)。

【0107】

そして、図16のステップC2において信頼度の更新が行われたとき、信頼度管理部701は、IPアドレスと、信頼度の更新に加えて、更新時刻をリアルタイム信頼度データベース7011に記録する。

【0108】

4.3) リアルタイム信頼度の複製処理
以上の処理に並行して、複製処理部7012は定期的に(例えば1日ごとに)リアルタイム信頼度データベース7011の全内容を走査しながら、各項目を長期信頼度データベース7013へコピーしていく。このとき、最終更新時刻を参照して、所定の期間(例えば1週間)以上、更新処理が行われなかった項目について、当該項目をリアルタイム信頼度データベース7011から削除する処理を行っても良い。

【0109】

4.4) 長期信頼度の更新処理

また、更新処理部 7014 は、定期的に（例えば 1 日ごとに）長期信頼度データベース 7013 の全内容を走査しながら、各項目の最終更新時刻を参照して、所定の期間（例えば 1 週間）以上、更新が行われなかった項目については、その信頼度を所定の値だけ減算する。もしくは、単に削除しても良い。

【0110】

4. 5) 効果

以上のような動作を行うことで、リアルタイム信頼度データベース 7011 の記憶容量を抑えることができるので、SDRAM など、低容量で高速な記憶デバイスを用いることができる。一方、長期信頼度データベース 7013 はアクセス頻度が少ないので、ハードディスクデバイスなど、大容量で低速な記憶デバイスを用いることができる。

【0111】

また、更新処理部 7014 による長期信頼度データベース 7013 の更新処理により、たとえ 1 度、十分な信頼度を得たソース IP アドレスについても、ある一定期間以上、アクセスが途絶えた場合には再び「不審」と見なすことができる。これは、特に中古 PC の売買など、ソース IP アドレスに相当するホストの利用環境が大きく変化した場合などに、信頼度の再評価を自動的におこなうことができるという効果をもつ。

【0112】

（第 5 実施形態）

本発明の第 5 実施形態として、図 23 に示す第 3 実施形態の信頼度管理部 502 に代えて、上述した第 4 実施形態の信頼度管理部 701 を用いたファイアウォール装置を構成することができる。基本的な構成は図 23 と同じであり、信頼度管理部 701 の構成及び動作は、図 24、図 25 および第 4 実施形態の項で説明した通りであるから、ここでは省略する。

【0113】

（第 6 実施形態）

6. 1) 構成

図 26 は、本発明の第 6 実施形態による攻撃防御システムのファイアウォール

装置 9 を示す概略的ブロック図である。ファイアウォール装置 9 では、第 1 実施形態のファイアウォール装置 1 における誘導部 103 に代えて、バッファ 901 1 および ICMP 監視部 901 2 を有する誘導部 901 が設けられている。本実施形態では、第 1 実施形態のように誘導リストを設けることなく、ICMP パケットを利用して同様の機能を実現できる。なお、簡略化のために、図 26 では他の機能ブロックの表示が省略されている。

【0114】

バッファ 901 1 は、次に述べるように、パケットフィルタ 101 より受け取ったパケットを一時的に蓄積し、第 1 内部通信インタフェース 105 を介して内部ネットワークへ転送すると共に、ICMP 監視部 901 2 からの求めに応じて、蓄積したパケットを第 2 の内部通信インタフェース 105 を介しておとり装置 2 へ再送信する。ICMP 監視部 901 2 は、第 1 の内部通信インタフェース 104 における ICMP パケットの受信を監視し、特定の ICMP エラーパケットを検出したとき、バッファ 901 1 に適切なパケット再送を要求する。以下、本実施形態の動作を詳述する。

【0115】

6. 2) 動作

図 27 は本実施形態によるファイアウォール装置 9 の動作を示すフローチャートである。まず、第 1 実施形態のファイアウォール装置 1 と同様に、外部通信インタフェース 100 を介してインターネット 4 から受信した入力 IP パケットについて、パケットフィルタ 101 によるフィルタリングを行う（ステップ A1, A2）。

【0116】

受理された IP パケットは誘導部 901 のバッファ 901 1 に蓄積され（ステップ E1）、無条件に第 1 の内部通信インタフェース 104 を介して内部ネットワーク 3 へ送出され（ステップ E2）、通常のサービスが提供される（ステップ A4）。この場合、たとえ不審パケットであっても内部ネットワークへ転送されてしまうが、実際の攻撃を実行する前に送信される TCP コネクション確立要求の SYN パケットは攻撃要素が含まれていないために、SYN パケットであれば

受け入れても問題はない。内部ネットワークにSYNパケットが転送され宛先が存在しなければ、到達不能を知らせるICMPパケット（タイプ3）が返される。

【0117】

ICMP監視部9012は、第1の内部通信インタフェース104でICMPパケット（RFC792記載）が受信されると、当該ICMPパケットの内容を参照して、到達不能を知らせるエラー（すなわちICMPタイプ3）であるか否かを調べる（ステップE3）。到達不能を知らせるエラーであれば（ステップE3のY）、そのIPヘッダ部をさらに参照し、少なくともソースIPアドレスもしくはデスティネーションIPアドレスを用いてバッファ9011に再送要求を行う（ステップE3）。その他のメッセージであった場合は、何もせず、監視を続ける。

【0118】

再送要求を受けたバッファ9011は、少なくともソースIPアドレスもしくはデスティネーションIPアドレスに従って、蓄積されたパケットから該当するパケットを抽出し、当該パケットを第2の内部通信インタフェース105を介して、おとり装置2へ再送する（ステップE4）。以下、すでに述べたステップA5～A8が実行される。

【0119】

このように攻撃要素を含まないコネクション確立のためのパケットを利用することで、内部ネットワーク3の未使用IPアドレスを誘導リストとして事前に設定することなしに、自動的に未使用IPアドレス宛ての入力IPパケットをおとり装置2へ誘導することができる。

【0120】

（第7実施形態）

7. 1) 構成

図28は、本発明の第7実施形態による攻撃防御システムのファイアウォール装置10を示す概略的ブロック図である。このファイアウォール装置10は、上述した第2～第5実施形態によるファイアウォール装置における防御ルール判定

部 107 およびアクセス制御リスト管理部 102 に代えて、有効期限付き防御ルール判定部 1001 および有効期限付きアクセス制御リスト管理部 1002 を設けている。

【0121】

防御ルール判定部 1001 は、制御インターフェース 106 を介しておとり装置 2 から受け取ったアラートに応じて、信頼度管理部 502 および 701 に対して、対応する信頼度の再設定を指示する。あるいは、アラートに応じて、更新すべきアクセス制御ルールを決定し、アクセス制御リスト管理部 1002 にその更新を指示する。

【0122】

信頼度管理部 502 および 701 は、防御ルール判定部 1001 からの更新指示を受けて、新たな信頼度を決定し誘導部 501 へ出力する。アクセス制御リスト管理部 1002 は、防御ルール判定部 1001 からの更新指示を受けて、アクセス制御リストを更新し、パケットフィルタ 101 からの要求に応じてアクセス制御ルールを出力する。

【0123】

7. 2) 動作

本実施形態における攻撃防御システムの動作を、具体的な例を挙げながら詳細に説明する。

【0124】

まず、インターネット 4 から到達した入力 IP パケットが、ファイアウォール装置 10 によって、おとり装置 2 へ誘導され、おとり装置 2 において、当該入力 IP パケットによる攻撃が検知され、その旨を知らせるアラートが送信されるまでは、図 16 のステップ A1～A7 に示すように、第 2～第 5 実施形態における攻撃防御システムと同様である。

【0125】

ファイアウォール装置 10 の防御ルール判定部 1001 には、防御ルール判定部 107 とは異なり、信頼度を更新するための防御ルールが予め設定されている。例えば、防御ルールとして、次式 (6) のような形式の記述があれば、信頼度

を1減算すると解釈されるものとする。

RECON: c (\$ {SOURCE__IP__ADDRESS}) -= 1
... (6)。

【0126】

たとえば、制御インタフェース106を通してソースIPアドレス「12. 34. 56. 78」を示すアラートが受け取ると、防御ルール判定部1001はIPアドレス「12. 34. 56. 78」に対する信頼度を1減算すると解釈し、その旨を信頼度管理部502/701に指示する。すなわち、アラートを受け取ると、そのソースIPアドレスの信頼度を低減させる。信頼度管理部502は第2実施形態で説明したように信頼度を更新し、信頼度管理部701は第4実施形態で説明したように信頼度を更新するから、信頼度の低減処理を加えることで、よりきめ細かい信頼度管理ができる。

【0127】

また、ファイアウォール装置10において、防御ルール判定部1001内に、防御ルール判定部107と同様に、アクセス制御ルールのひな型としての防御ルールを予め設定してもよい。ただし、この場合のアクセス制御ルールは、新たに「有効期間」を表すフィールドを記載できる（したがって防御ルールにも記載可能）。例えば、次式(7)に示すように、前記式(1)の防御ルールにEXPIREの項を追加し、「7日間有効」という制約をつけることができる。

INTRUSION: (SRC: \$ {SOURCE__IP__ADDRESS} ,
DST: *, PROC: DROP, EXPIRE: +7DAY) ... (7)

。

【0128】

したがって、アラートが制御インタフェース106を経由して防御ルール判定部1001に伝達されると、防御ルール判定部107と同様の方法で、次式(8)に示すようにアクセス制御ルールが生成され、アクセス制御リスト管理部1002に伝達される。

(SRC: 12. 34. 56. 78, DST: *, PROC: DROP, EXPIRE: +7DAY) ... (8)。

【0129】

次に、アクセス制御リスト管理部1002は、防御ルール判定部1001から受け取ったアクセス制御ルールをアクセス制御リストデータベース1021に追加する。このとき、式(8)のようにEXPIREフィールドがアクセス制御ルールに記載されている場合、アクセス制御リスト管理部1002は、現在時刻に、EXPIREフィールドに指定された値を加算した時刻を算出した上で、データベースを更新する(図7のステップA8に対応する)。

【0130】

図29は、アクセス制御リスト管理部1002の管理動作を示すフローチャートである。アクセス制御リストデータベース1021が更新された後、再びソースアドレス「12.34.56.78」からの入力IPパケットがファイアウォール装置10に到達すると、パケットフィルタ101は当該ソースIPアドレスをアクセス制御リスト管理部1002へ送付してアクセス制御ルールの取得要求を行う(ステップA2__1)。

【0131】

アクセス制御リスト管理部1002は、当該ソースIPアドレスに対応するアクセス制御ルールを検索する(ステップA2__2、A2__3)。式(8)に相当するアクセス制御ルールを抽出すると、アクセス制御リスト管理部1002は、EXPIREフィールドに記載された有効期間と現在時刻とを比較する(ステップA2__4)。

【0132】

現在時刻が有効期間を超過していた場合には(ステップA2__4のYES)、当該アクセス制御ルールをアクセス制御リストデータベース1021から削除し(ステップA2__5)、デフォルトのアクセス制御ルールをパケットフィルタ101へ返す(ステップA2__6)。逆に、有効期間内であれば(ステップA2__4のNO)、次式(9)に示すようなEXPIREフィールドを除いたアクセス制御ルールをパケットフィルタ101へ返す(ステップA2__7)。

(SRC:12.34.56.78, DST:*, PROC:DROP)

... (9)。

【0133】

こうして取得したアクセス制御ルールを用いて、パケットフィルタ101は受信IPパケットの受理／廃棄の判定を行う（ステップA2）。

【0134】

上述したように、攻撃をおとり装置で検知した後の防御方法として、よりきめ細かな対策を講じることができる。具体例を挙げると、一般に攻撃者は、「侵入」もしくは「破壊」に相当する攻撃の準備として、ポートスキャンあるいはTracerouteなどの「探査」に相当する攻撃を行う。しかし、「探査」として検出されるアクセスが、全て攻撃であるとは限らないことも、よく知られる所である。したがって、「探査」に対する防御方法として、恒久的なアクセス遮断を行うことは不都合を生じる可能性がある。

【0135】

そこで、本実施形態では、有効期限付きのアクセス制御ルールを用いて時間制限を付けたアクセス遮断を行う。または、上述したように、アラーム発生によってそれまで蓄積された信頼度を低減させることで、信頼度がしきい値T（図17参照）を超えないようにし、おとり装置への誘導を継続し、後で「侵入」もしくは「破壊」に相当する攻撃を検知してから恒久的なアクセス遮断へと対応を変えることもできる。

【0136】

（第8実施形態）

図30は、本発明の第8実施形態による攻撃防御システムの概略的構成図である。第8実施形態では、単一のおとり装置2に代えて、2台以上のおとり装置2を含むおとりクラスタ21が設けられている。

【0137】

本実施形態における各おとり装置2は、特定のディスティネーションIPアドレスをもつパケット、もしくは、特定のポート番号をもつパケットにしか偽のサービスを提供しないようにする。

【0138】

こうすることにより、内部ネットワーク4上の特定のサーバ装置に1対1対応

するおとり装置 2 を設けたり、特定の偽のサービスだけを提供するおとり装置 2 を設けたりすることができる。したがって、攻撃者に対して正規のサーバ装置により近いサービスを提供することができ、また、特定のサービス向けの正常動作定義をもつことでより運用性を向上させることもできる。

【0139】

(第 9 実施形態)

第 9 実施形態のファイアウォール装置は、第 1 ～第 8 実施形態における誘導部に加えて、出力パケット誘導部を有する。出力パケット誘導部は、内部ネットワーク 3 からインターネット 4 へ向けて送信される出力 IP パケットに対して、上述したパケットフィルタリングおよびおとり装置への誘導処理を行う。

【0140】

このような出力パケット誘導部を設けることで、内部ネットワーク 3 の運用規定として、インターネット 4 へのアクセスを禁じているような場合に、内部ネットワーク 3 からインターネット 4 への不法なアクセスを検知し、その記録をとることができる。

【0141】

(第 10 実施形態)

上記第 1 ～第 9 実施形態の説明では機能ブロック構成を用いたが、本発明はこれに限定されるものではなく、ソフトウェアにより同一の機能を実現することもできる。

【0142】

図 31 は、本発明の第 10 実施形態による攻撃防御システムの概略的構成図である。本実施形態のファイアウォール装置には、プログラム制御プロセッサ 1101、上記第 1 ～第 9 実施形態におけるそれぞれの機能ブロックを実現するプログラムのセットを格納したプログラムメモリ 1102、アクセス制御リストデータベースや防御ルール判定用のデータベースなどを格納したデータベース 1103、および各種インタフェース 100、104 ～106 が設けられている。同様に、本実施形態のおとり装置には、プログラム制御プロセッサ 2101、上記第 1 実施形態で説明したおとり装置としての機能ブロックを実現するプログラムの

セットを格納したプログラムメモリ 2102 およびファイアウォール装置とのインタフェースが設けられている。本実施形態の動作は、プログラムメモリに格納されるプログラムセットを上記第1～第9実施形態のいずれかに設定することで、所望の実施形態による攻撃防御システムを実現することができる。

【0143】

(第11実施形態)

上記第1～第10実施形態では、ファイアウォール装置とおとり装置とが別ユニットになった攻撃防御システムを例示したが、本発明はこれに限定されるものではなく、ハードウェア的に1ユニットで構成することもできる。1ユニットは、取り扱いが容易であり小型化し易いというメリットがある。

【0144】

図32は、本発明の第11実施形態による攻撃防御ユニットの概略的構成図である。本実施形態の攻撃防御ユニットには、ファイアウォール装置用のプログラム制御プロセッサ1101、おとり装置用のプログラム制御プロセッサ2101、アクセス制御リストデータベースや防御ルール判定用のデータベースなどを格納したデータベース1103、上記第1～第9実施形態におけるそれぞれの機能ブロックを実現するプログラムのセットを格納したプログラムメモリ1104、および各種インタフェース100および104が設けられている。本実施形態の動作は、プログラムメモリに格納されるプログラムセットを上記第1～第9実施形態のいずれかに設定することで、所望の実施形態による攻撃防御システムを実現することができる。また、プロセッサ1101とプロセッサ2101とを単一のプロセッサで構成しても良い。

【0145】

(第12実施形態)

12. 1) 構成

図33は、本発明の第12実施形態によるおとり装置のブロック図である。本実施形態におけるおとり装置37は、第1～第10実施形態におけるおとり装置2の攻撃検知部202に代えて、イベント管理部3701および攻撃検知部3702を備える。

【0146】

イベント管理部3701は、プロセッサ201から伝達されるプロセス状況（以下イベント）を内部的に備えたキューに一時格納しながら、所定の条件を満たす関係をもつ過去のイベントとの間にリンク付けを行い、当該イベントとリンクを攻撃検知部3702に伝達する。また、攻撃検知部3702からリンクの入力を受けて、リンク先またはリンク元イベントを返す。

【0147】

攻撃検知部3702は、イベントとリンクの組の伝達を受けて、必要に応じて、イベント管理部3701を用いてリンクを探索しながら、所定の攻撃検知ルールとの照合によって攻撃の有無を判定し、攻撃があった場合にファイアウォール装置にその旨を通知するためのアラームを送信する。

【0148】

12. 2) 動作

図34は、本発明の第12実施形態によるおとり装置37の動作を示すフローチャートである。

【0149】

12. 2. 1) イベント伝達

まず、ファイアウォール装置1から転送された入力IPパケットを受けて、プロセッサ201上の偽サービスを提供するためのプログラムが動作する。第1～第10実施形態におけるおとり装置2とは異なり、この偽サービス提供は正規のサービス提供と全く同じように、ネットワーク入出力・プロセスの生成と停止（プロセス生滅）・ファイル入出力を行うものとする。

【0150】

プロセッサ201は、当該プログラムを動作させながら、さらに、ネットワーク入出力・プロセス生滅・ファイル入出力に係るイベントを、イベント管理部3701に随時伝達する（ステップF1）。

【0151】

イベントには、少なくとも、イベント名および引数の値や、イベントの返値や、当該イベントを発行したプロセスのプロセスIDが含まれる。この他、イベン

トの発生時刻などを含めてもよい。

【0152】

12.2.2) イベント種別の判定

イベントの伝達を受けたイベント管理部3701では、まず所定のイベント種別判定ルールに従って、イベント種別を判定する(ステップF2)。イベント種別判定ルールは、少なくともネットワーク入出力・プロセス生滅・ファイル入出力を区別できれば十分である。たとえば、プロセッサ201が伝達するイベントの名前と、イベント種別との対応関係を定めたテーブル(図35参照)を予め用意しておき、イベントが伝達されるたびに当該テーブルを検索して、イベント種別を導けばよい。

【0153】

12.2.3) イベント管理キューへの追加

そして、イベント管理部3701は、前記イベントをキューに格納する(ステップF3)。キューは1本でもよいが、並列処理や後段の処理を簡単にするために、複数本を備えてもよい。ここでは、たとえば、イベント種別ごとに1本ずつのキューを備えるものとする(図36参照)。この場合、前記イベント種別判定ルールによって求められたイベント種別について、対応するキューを選択し、その最後尾に前記イベントを追加する。

【0154】

12.2.4) イベント間のリンク付け

さらに、イベント管理部3701は、最後にキューに追加したイベント(カレントイベント)について、所定のリンク付けルールにしたがって、関連イベントとの間にリンク付けを行う(ステップF4)。リンク付けルールは、少なくともイベントの発生源となったプロセスの生成イベントから、当該イベントへのリンクを生成できれば十分である(図43参照)。

【0155】

12.2.4.1) 基本的なリンク付けルール

図37を参照しながら、より具体的な例として、もっとも基本的なリンク付けルールを示す。

【0156】

図37において、まず、前記カレントイベントの発行源プロセスIDを抽出する（ステップH1）。そして、プロセスイベント管理キューの最後尾にあるイベントを参照する（ステップH2）。

【0157】

次に、現在参照しているイベントが、プロセス生成イベントか否かを判別する（ステップH3）。具体的には、例えば、予め定めたイベント名と、現在参照中のイベントに記載されたイベント名が一致するかどうかを検査する。

【0158】

そして、プロセス生成イベントではないと判定された場合は、参照先を1つ前方に移動させ、ステップH3へ戻る（ステップH4）。

【0159】

一方、プロセス生成イベントであると判定された場合は、現在参照しているイベントのプロセスIDを参照して、前記発行源プロセスIDと比較する（ステップH5）。一致する場合は、ステップH6に進み、一致しない場合は、ステップH4に戻る。

【0160】

なお、カレントイベントがプロセス生成イベントである場合、ステップH2で参照されるイベントはカレントイベント自身である。しかし、どのオペレーティングシステムにおいても、プロセス生成の際に、同じプロセスIDが割り当てられることはあり得ない。したがって、ステップH5において、カレントイベントの発行源プロセスIDと、カレントイベントのプロセスIDは一致せず、必ずステップH4へ戻る。

【0161】

そして、当該プロセス生成イベントから、カレントイベントへの、順方向リンクをプロセス生成イベントに付加する（ステップH6）。さらに、カレントイベントからプロセス生成イベントへの、逆方向リンクをカレントイベントに付加する（ステップH7）。順方向および逆方向のリンクの一例は図43に示される。

【0162】

こうして付加された順方向リンクは、イベント間の関係を時系列に沿った形で保持するためのものであり、逆方向リンクは、イベント間の関係を時系列とは逆順に保持するためのものである。以降の処理において、イベント間の時間的な関係を利用するので、同じイベントに付加された、順方向リンクと逆方向リンクはいつでも区別できるようにしておくことが望ましい。

【0 1 6 3】

1 2. 2. 4. 2) イベントーコンテキスト対の伝達

その後、イベント管理部 3 7 0 1 は、前記カレントイベントと、そのコンテキストとの組（イベントーコンテキスト対）を攻撃検知部 3 7 0 2 に入力する。図 3 8 に示すように、コンテキストとは、カレントイベントに付加された全ての順方向リンクおよび逆方向リンクの集合を指す。

【0 1 6 4】

1 2. 2. 5) 攻撃検知

図 3 9 に、予め定められたドメインータイプ制約付きの正常動作定義（以下、D T 定義という。）の一例を示す。イベントーコンテキスト対の入力を受けた攻撃検知部 3 7 0 2 は、D T 定義にしたがって攻撃の有無を判定する（図 3 4 のステップ F 5）。

【0 1 6 5】

1 2. 2. 5. 1) ドメインータイプ制約つきルールの判定

（ドメインータイプ制約つきルールの構成要素）

D T 定義内の各ドメインータイプ制約つきルールは、少なくとも、

- （1）ドメインータイプ制約（以下、D T 制約）
- （2）イベント制約
- （3）判定値

という構成要素をもつ。

【0 1 6 6】

（1）D T 制約は、イベントの発生原因となったアクセスの送信元ホストもしくはそのネットワークドメインに関する制約（ドメイン制約）と、イベントの発生源となったプロセスおよびその先祖プロセスに関する制約（タイプ制約）とを

論理積で組み合わせた制約条件を示しており、前記イベントがこの制約を満たす場合のみ、(2) イベント制約の判定を行う。

【0 1 6 7】

D T 制約について、より具体的に説明する。たとえば、以下のように D T 制約が記述されているものとする。

【0 1 6 8】

- ・ タイプ制約：「プログラム T 1」「プログラム T 2」
- ・ ドメイン制約：「1 3 3. 2 0 3. 1. 1 2 8」。

【0 1 6 9】

図 4 0 に示すように、これらの制約は以下の条件を指定する。

- ・ イベントの発生源である何らかのプロセスの先祖として、「プログラム T 2」のプロセスが存在すること。
- ・ 「プログラム T 2」の親プロセスとして「プログラム T 1」のプロセスが存在すること。
- ・ 「サーバプログラム」が IP アドレス「1 3 3. 2 0 3. 1. 1 2 8」のホストからアクセスを受けていること。

【0 1 7 0】

なお、図 4 0 は「サーバプログラム」が「プログラム T 1」の先祖である場合を示しているが、一般的にはイベント発生源のプロセスおよびその先祖プロセスのいずれかが「サーバプログラム」であれば十分である。たとえば、「プロセス T 1」または「プロセス T 2」が「サーバプログラム」であってもよいし、イベント発生源のプロセスそのものが「サーバプログラム」であってもよい。

【0 1 7 1】

(2) イベント制約と (3) 判定値は、第 1 実施形態におけるおとり装置 2 の正常動作定義と同じ意味である。すなわち、前記 (2) はイベント名とパラメータ値についての正規表現の組である。攻撃検知部 3 7 0 2 は、それらが前記イベントーコンテキスト対におけるイベントの名前およびパラメータ値と、合致するかどうかを判定する。

【0 1 7 2】

また、前記（3）は、前記イベントが前記（2）に合致した場合に、攻撃検知部 3 7 0 2 がそれを正常と判定するか、攻撃と判定するか、を定める値である。たとえば、正常と判定する場合の判定値を「ALLOW」、攻撃と判定する場合の判定値を「DENY」とする。なお、攻撃と判定する場合の判定値については、第 1 実施形態におけるおとり装置 2 と同様の攻撃種別を用いても良い。

【0 1 7 3】

以下、特に D T 制約について、より具体的な記述例と判定方法を示す。

【0 1 7 4】

（ドメイン制約の記述例）

ドメイン制約は、例えば、I P アドレスの集合として記述できる。具体的には、1 つの I P アドレスを 10 進 3 桁の数の 4 組「xxx.yyy.zzz.www」として記述し、「.」で区切って I P アドレス集合の要素を列挙する。またその便法として、「xxx.yyy.zzz.www/vvv」（vvv はビットマスク）などの表記を許してもよい。あるいは、正規表現を用いることもできる。

【0 1 7 5】

（タイプ制約の記述例）

また、タイプ制約は、例えば、実行形ファイル名に関する正規表現をもちいて記述できる。また、実行形ファイル名の連結によって、プロセスの親子関係を表現できるようにして、その正規表現を用いてもよい。

【0 1 7 6】

具体的には、プロセスの親子関係を「<F(1)><F(2)>(中略)<F(N)>」（各 F(i) は実行形ファイル名）という形式で表すことができる。このとき、それぞれの「<F(i)>」は、プロセスに関する制約であり、これにマッチする名前をもつ実行形ファイルの起動後のプロセスに相当する。また、その列挙は前方に記述されたプロセスを親とし、後方に書かれたプロセスをその直接の子とすることを示す。

【0 1 7 7】

したがって、実行形ファイル「A」に相当するプロセス A の子として、実行形ファイル「B」に相当するプロセス B が、さらにその子として実行形ファイル「C」に相当するプロセス C が起動されている場合、プロセス A、B、C の親子関

係は「<A><C>」という文字列で表記される。

【0178】

こうしたプロセスの親子関係に関する正規表現をもって、タイプ制約とすることができる。具体的には、「<A>.*<C>」というタイプ制約は、実行形ファイル「C」に相当するプロセスCが起動しており、その親プロセス（直接でなくともよい）が実行形ファイル「A」である場合に、マッチする。

【0179】

また特殊な例として、タイプ制約が「^」で始まる場合、その直後に記述されたプロセスが、プロセッサ201上のオペレーティングシステムの起動直後に生成されたプロセスである場合にマッチする。

【0180】

一般に、オペレーティングシステムは、唯一の初期プロセスをもち、起動直後のプロセスはすべて、その初期プロセスの直接の子となる。初期プロセスに相当する実行形ファイルが必ずしも存在するわけではないので、これを特殊記号「^」で表記することで、DT定義の汎用性を向上させることができる。

【0181】

別の特殊な例として、タイプ制約が「\$」で終わる場合、「\$」の直前に指定されたプロセス「<F(N)>」が、イベント発生源であることを示す。

【0182】

（DT制約とイベントーコンテキスト対の比較）

DT制約の判定において、前記イベントーコンテキスト対との比較を行うが、その方法について、詳細に説明する。

【0183】

タイプ制約の判定は、コンテキストに含まれる逆方向リンクのうち、前記プロセスイベント管理キュー内のイベントを指すもの（以下、プロセスリンク）を選択する。前記リンク付けルールに従えば、任意のイベントにはその発生源であるプロセスの生成イベントを指すプロセスリンクが必ず存在する。

【0184】

そして、当該プロセスリンクを辿り、その先のイベントを参照して、実行形フ

ファイル名をスタックに積む。こうしたステップを、プロセスリンクが存在しないイベントに到達するまで繰り返す。

【0185】

一般的なオペレーティングシステムでは、任意のプロセスの先祖として初期プロセスが存在する。そのようなオペレーティングシステムがプロセッサ 2 0 1 上で動作している場合、初期プロセスは親プロセスをもたないため、かならず本ステップの繰り返しは終了する。

【0186】

もし、初期プロセスが存在しないようなオペレーティングシステムがプロセッサ 2 0 1 上で動作している場合、イベント管理部 3 7 0 1 において、仮想的な初期プロセスの生成イベントを、プロセスイベント管理キューの先頭に配置するようにすればよい。

【0187】

前記ステップが終了した後、スタックに積まれた実行形ファイル名の系列は、前記初期プロセスから、前記イベント発生源のプロセスに至るまでのプロセス系列が得られる。当該プロセス系列は、プロセス間の親子関係を時系列順にならべたものに一致するので、当該プロセス系列と、タイプ制約とを比較することで、イベント系列とタイプ制約が合致するか否かを判定できる。

【0188】

また、ドメイン制約の判定は、タイプ制約と同様にプロセスリンクをたどりながら、順次ネットワークイベント管理キューへの順方向リンクを参照していく。順方向リンクの先に、接続要求の受信イベントが見つければ、当該イベントに記載されているソース IP アドレスをアクセス元ホストの IP アドレスとみなし、探索を終了する。

【0189】

そして、前記 IP アドレスと、ドメイン制約とを比較して合致するか否かを判定する。

【0190】

1 2 . 2 . 5 . 2) アラーム送信

以上のようにして、イベントーコンテキスト対と D T 定義に記載された各ルールとの照合を繰り返し行い、前記 (1) D T 制約、 (2) イベント制約の全てに合致するかどうかを確認する (図 3 4 のステップ F 6) 。

もし、両方の制約に合致するルールが 1 つも無い場合は、デフォルト値として予め D T 定義内に設定された判定値を採用する。

【 0 1 9 1 】

合致するルールがあれば、当該ルールの (3) 判定値を参照して、前記イベントーコンテキスト対が攻撃であるかどうかを判定する (ステップ F 7) 。

【 0 1 9 2 】

そして、採用された判定値が許可 (A L L O W) 以外の場合、ただちにアラームを生成し、ファイアウォール装置 1 に送信する (ステップ F 8) 。アラームの内容は第 1 実施形態におけるおとり装置 2 と同様に、少なくとも、前記アクセスのソース I P アドレスと、前記判定値を含み、その他、アクセス元のポート番号などを含めても良い。

【 0 1 9 3 】

1 2 . 3) 効果

本実施形態におけるおとり装置 3 7 は、プロセッサ 2 0 1 が発生するイベントについて、イベント管理部 3 7 0 1 でイベント間の因果関係の分析と履歴管理を行っている。これを用いて、攻撃検知部 3 7 0 2 でアクセス元ホストや、サブシステムの呼び出し関係などを含めた、より詳細な正常動作定義が可能となる。これにより、複雑なサブシステム構成をもつサーバに対する攻撃検知性能を向上させると共に、保守作業の誤検知を低減させることができる。

【 0 1 9 4 】

1 2 . 4) 具体例

本実施形態におけるおとり装置 3 7 の動作を具体例を用いて説明する。

【 0 1 9 5 】

1 2 . 4 . 1) 構成

まず、おとり装置 3 7 のプロセッサ 2 0 1 上で、偽サービスとして WWW サーバが動作しているものとする。そして、そのコンテンツ領域を、 " C : ¥ I n e t p u b ¥ w w

wroot” ディレクトリ以下とする。

また、WWWサーバのサブシステムとして、以下の2つのCGIモジュールを備えるものとする。

【0196】

(A) 登録CGI：顧客情報を顧客データベースに登録するCGI

(パス名：“C:\Inetpub\scripts\regist.exe”)

(B) 出力CGI：顧客データベースの内容をHTMLに変換し、ブラウザから閲覧するCGI

(パス名：“C:\Inetpub\scripts\view.exe”)。

【0197】

ただし、出力CGIは専ら保守作業の1つとして利用されることを目的としており、内部ネットワーク4上の管理ドメイン”10.56.3.0/24”からのアクセスのみに応答することを要求されているものとする。また、別の保守作業として、FTPサーバを介したコンテンツの更新が想定されているものとする。

【0198】

以下、クライアントとサーバとの間で行われる接続開始から要求データ送信完了までのIPパケット送受信をまとめて「アクセス」と呼ぶ。同様に、応答データ送信開始から接続終了までのIPパケット送受信をまとめて「(当該アクセスに対する) 応答」と呼ぶ。

【0199】

こうした構成に対するDT定義の例として、図39に示すファイル4101のような設定がなされているものとする。ただし、「#」で始まる行はコメント行であり、無視されるものとする。

【0200】

12.4.2) 動作例1

具体的な動作の一例として、外部ネットワーク3上のクライアント(133.201.57.2)から、内部ネットワーク4上のWWWサーバに対する不審アクセスがあつて、それが正常である場合のおとり装置37の動作例を示す。

【0201】

このとき、第1～第10実施形態のいずれかのファイアウォール装置によって、前記不審アクセスはおとり装置37に誘導され、偽サービス処理が開始される。

【0202】

そして、おとり装置37のプロセッサ201上のWWWサーバでは、前記不審アクセスを受信を初めとして、以下のような処理を行う。

- (A) 133.201.57.2からのアクセスを受信する。
- (B) 子プロセスを生成する。
- (C) 子プロセスで、当該アクセスにおける要求データに応じて、

例えば、

(C-1) コンテンツ領域に対するファイル入出力

(C-2) データベース操作のためのファイル入出力

を行う。

【0203】

以下に、それぞれのステップごとにおとり装置37の内部動作を説明する。

【0204】

12.4.2.1) 不審アクセスの受信

プロセッサ201上のWWWサーバが、不審アクセスを受信した直後、プロセッサ201からイベント管理部3701に、イベント3501が伝達される(図41参照)。

【0205】

イベント3501の内容には、少なくとも、イベント名(NW_ACCEPT)、アクセス元IPアドレス(133.201.57.2)、当該イベントの発生源であるプロセスであるWWWサーバのプロセスID(709)が記載される。その他、アクセス元のポート番号、TCP/UDPなどのプロトコル種別、要求データなどの情報を含めてもよい。

【0206】

イベント3501を受け取ったイベント管理部3701は、直ちに図35に示すような対応表を参照して、イベント名「NW_ACCEPT」のイベント種別

を「ネットワーク」であると判定し、前記イベントに追記する。そして、イベント種別「ネットワーク」に対応するイベント管理キューに、イベント3501を追加する。さらに、所定のリンク付けルールに従いイベント3501と関連する過去のイベントとの間にリンク付けを行う。

【0207】

具体的には、図42を参照すると、イベント種別「プロセス」に対応するイベント管理キューから、前記イベント内に記載されたプロセスID(709)に相当するイベント名「PROC_EXEC」または「PROC_FORK」をもつイベント3601を検索する。このとき、最後尾から前方に向けてキュー走査を行い、最初にマッチするイベント3601を発見したとき、後の処理へ進む。

【0208】

そして、イベント3601に対して、イベント3501への順方向リンク(図43の実線)を付加し、イベント3501に対して、イベント3601への逆方向リンク(図43の破線)を付加する。以下、リンクを図示する際は、逆方向リンクを省略する。

【0209】

その後、イベント3501に関するイベントーコンテキスト対を、攻撃検知部3702に伝達する。

【0210】

攻撃検知部3702では、まず、所定のDT定義ファイル4101を参照し、各ルールを抽出する。本例では、DT定義ファイル4101の先頭から前方に向かって1行ずつルールを抽出していく。なお、「#」で始まる行はコメントを意味し、コメントと空行はスキップされる。

【0211】

まず、最初のルール(図39のルール1)が抽出される。本例の場合、ドメイン制約は「0.0.0.0/0」であり、これは任意のネットワークドメインにマッチする。また、タイプ制約は「<inetinfo.exe>」であり、WWWサーバに相当するプロセスまたはその子プロセスにマッチする。

【0212】

前記DT制約とイベント3501との照合のために、攻撃検知部3702は、まず、イベント3501のコンテキスト内の逆方向リンクをイベント管理部3701に入力して、リンク先のイベント3601の出力を受ける。

【0213】

次に、イベント3601の内容を参照して、プロセスID「709」に相当するプログラム実行形ファイルのパス名「C:\Web\inetinfo.exe」を抽出する。さらに、イベント3601の逆方向リンクを先と同様にして、さらに親プロセスの生成イベントの取得を行おうとするが、本例では存在しない。したがって、イベント3601に相当するプロセスの親子関係を「<inetinfo.exe>」と判定し、前記タイプ制約「<inetinfo.exe>」にマッチすることを確認する。

【0214】

次に、ドメイン制約との照合を行うため、再びイベント3501の内容を参照する。まず、イベント3501のイベント種別が「ネットワーク」であることを確認して、さらにイベント名が「NW_ACCEPT」であることを確認する。これにより、イベント3501自身がドメイン制約の対象となるので、さらにソースIPアドレスを参照して、「133.201.57.2」を取得する。この値は、前記ドメイン制約「0.0.0.0/0」にマッチする。

【0215】

続けて、イベント制約の判定を行う。イベント名「FILE_WRITE」と、イベント3501のイベント名「NW_ACCEPT」とを照合するが、この場合、一致しないので、当該ルール of 照合処理を中断し、次のルール照合へ移る。

【0216】

以下、同様にして、ルール抽出、DT制約の照合、イベント制約の照合を繰り返すが、本例の場合、いずれのルールにも合致しないため、デフォルトルール「DEFAULT;ALLOW」が採用され、イベント3501を「正常」と判定し、DT定義全体の照合を終了する。

【0217】

12.4.2.2) 子プロセスの生成

次に、プロセッサ201上のWWWサーバは前記不審アクセスの要求データを

処理するために、子プロセスを生成する。一般に複数のアクセスを並行処理するサーバは、このように個々のアクセスに対する要求データ処理と応答処理を子プロセス側で行う。ただし、逐次的にアクセスを処理するサーバもあり、こうした場合には、直ちに要求データの処理に移る。また、子プロセスの代わりに子スレッドを作る場合もあるが、本例ではスレッドと厳密な意味でのプロセスとを同等に、「(広義の) プロセス」として扱う。

【0218】

プロセッサ201は、子プロセスの生成動作を受けて、イベント3801(図44参照)をイベント管理部3701に伝達する。イベント3801の内容には、少なくとも、イベント名「PROC_FORK」と、実行形ファイルのパス名「C:\Web\inetinfo.exe」と、生成された子プロセスのプロセスID(800)と、当該イベントの発生源であるプロセスID(709)が記載される。この他、スレッドと(狭義の) プロセスを区別するためのフラグなどを設けてもよい。

【0219】

イベント3801の伝達を受けたイベント管理部3701は、前記イベント3501と同様にして、イベント3801のイベント種別(「プロセス」)を判定し、プロセスイベント管理キューへイベント3801を追加した後、イベント3601からイベント3801への順方向リンクと、イベント3801からイベント3601への逆方向リンクをつける(図44参照)。そして、イベント3801に関するイベントーコンテキスト対を攻撃検知部3202へ伝達する。

【0220】

攻撃検知部3702では、先と同様に、イベント3801に関するイベントーコンテキスト対のリンクを探索して、イベント3801のDT判定を行う。その結果、イベント3801そのものがイベント種別「プロセス」であり、イベント3801の逆方向リンク先をイベント管理部3201から取得すると、イベント3601が得られる。したがって、イベント3801のタイプは「<inetinfo><inetinfo>」と判定される。

【0221】

そして、再びイベント3801を参照するが、そのイベント種別は「ネットワ

ーク」ではないので、イベント 3801 の順方向リンクを参照しようとする。しかし、イベント 3801 にはネットワークイベント管理キューへの順方向リンクがないので、イベント 3801 の逆方向リンク先をイベント管理部 3701 から取得する。イベント 3801 にはネットワークイベント管理キューへの順方向リンクがあるので、さらにその先にあるイベント 3501 を、イベント管理部 3201 から取得する。イベント 3501 は、イベント名が「NW_ACCEPT」、ソース IP アドレスが「133.201.57.2」であるので、イベント 3801 のドメインを「133.201.57.2」と判定する。

【0222】

なお、本例のように、プロセスの生成に係るイベントのドメイン決定時には、特別にその旨をイベント管理部 3701 に伝達して、イベント 3801 からイベント 3501 への逆方向リンクを付加するようにしてもよい。このようにすることで、WWWサーバが子プロセスの実行中に、新たなアクセスを受信した場合でも、当該子プロセスが発生する後続イベントのドメインを誤ることはない。

【0223】

次に、DT 定義ファイル 4401 との照合を行うが、本例の場合、イベント 3501 と同様に、イベント 3801 は、いずれのルールにも完全に合致することなく、デフォルトの判定値（「DEFAULT; ALLOW」）が採用されるので、「正常」と判定される。

【0224】

12.4.2.3) コンテンツ領域に対するファイル入出力

次に、プロセッサ 201 上の WWWサーバの子プロセスは前記不審アクセスの要求データを処理する。ここでは、まず、当該要求データが「GET /HTTP/1.0」である場合の動作例を示す。

【0225】

前記要求データに対して、前記子プロセスは、コンテンツ領域内のファイル「C:\Inetpub\wwwroot\default.htm」を読み込む。この動作を受けて、プロセッサ 201 はイベント 3901（図 45 参照）をイベント管理部 3701 に伝達する。イベント 3901 の内容には、少なくとも、イベント名「FILE_READ

」、読み込むファイルのパス名「C:¥Inetpub¥wwwroot¥default.htm」、当該イベントの発生源である子プロセスのプロセスID（800）が記載される。この他、実際に読み込んだファイル内容などを含めても良い。

【0226】

次に、イベント管理部3701は、イベント3901のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント3901を追加する。その後、イベント3801からイベント3901への順方向リンクと、イベント3901からイベント3801への逆方向リンクを付加する（図45参照）。その後、イベント3901に関するイベントーコンテキスト対を攻撃検知部3202に伝達する。

【0227】

そして、攻撃検知部3702は、イベント3901に関するイベントーコンテキスト対に対するDT判定を行う。その結果、イベント3901のタイプを「<inetinfo.exe><inetinfo.exe>」、ドメインを「133.201.57.2」と判定する。

【0228】

次に、攻撃検知部3702は、DT定義ファイル4101との照合を行う。本例の場合、以下のルール（図39のルール2）に合致し、その判定値が「ALLOW」であることから、「正常」と判定される。

【0229】

0.0.0.0/0, <inetinfo.exe>, FILE_READ, C:¥Inetinfo¥.*;

ALLOW

【0230】

12.4.2.4) データベース操作

別の要求データの例として、「GET /cgi-bin/regist.exe?name=someoneHTTP/1.0」である場合の動作例を示す。

【0231】

(ア) CGIの起動

この要求データに対して、前記子プロセスは、まず、前記登録CGIを起動し

て、新たな孫プロセスを生成する。また、URLパラメータ「name=someone」は環境変数「QUERY_STRING」に格納されているものとする。

【0232】

この動作を受けて、プロセッサ201はイベント4001（図46参照）をイベント管理部3701に伝達する。イベント4001の内容には、少なくとも、イベント名「PROC_EXEC」と、実行形ファイルのパス名「C:\Inetpub\scripts\reglist.exe」と、前記孫プロセスのプロセスID（801）と、当該イベントの発生源である前記子プロセスのプロセスID（800）とが記載される。この他、環境変数の情報などを含めてもよい。

【0233】

次に、図46を参照すると、イベント管理部3701は、イベント4001のイベント種別を「プロセス」と判定し、プロセスイベント管理キューにイベント4001を追加する。その後、イベント3801からイベント4001への順方向リンクと、イベント4001からイベント3801への逆方向リンクを付加し、イベント4001に関するイベントーコンテキスト対を攻撃検知部3702に伝達する。

【0234】

そして、攻撃検知部3702は、イベント4001に関するイベントーコンテキスト対に対して、イベント3901と同様にDT判定を行う。その結果、イベント4001のタイプを「<inetinfo.exe><inetinfo.exe><reglist.exe>」、ドメインを「133.201.57.2」と判定する。

【0235】

次に、攻撃検知部3702は、DT定義との照合を行う。本例の場合、合致するルールがないので、デフォルトルールの判定値「ALLOW」を採用して、正常と判定する。

【0236】

（イ）CGIの動作

続けて、前記登録CGIがデータベース出力を行う。本例では、登録CGIが操作するデータベースを「C:\data\client.db」ファイルとする。

【0237】

データベース出力の具体例として、登録CGIは前記環境変数「QUERY_STRING」の値を読み取り、その値「name=someone」に改行記号を加えた文字列を前記データベースの末尾に追記するものとする。

【0238】

この動作を受けて、プロセッサ201はイベント4101（図47参照）をイベント管理部3701に伝達する。イベント4101の内容には、少なくとも、イベント名「FILE_WRITE」と、実行形ファイルのパス名「C:¥data¥client.db」と、当該イベント発生源である前記孫プロセスのプロセスID（801）とが記載される。この他、書き出したデータの内容などを含めてもよい。

【0239】

次に、図47を参照すると、イベント管理部3701は、イベント4101のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント4101を追加する。その後、イベント4001からイベント4101への順方向リンクと、イベント4101からイベント4001への逆方向リンクを付加し、イベント4101に関するイベントーコンテキスト対を攻撃検知部3702に伝達する。

【0240】

そして、攻撃検知部3702は、イベント4101に関するイベントーコンテキスト対に対して、DT判定を行う。その結果、イベント4101のタイプを「<inetinfo.exe><inetinfo.exe><regist.exe>」、ドメインを「133.201.57.2」と判定する。

【0241】

次に、攻撃検知部3702は、DT定義ファイル4101との照合を行う。本例の場合、以下のルール（図39のルール3）に合致するので、その判定値「ALLOW」を採用して、正常と判定する。

【0242】

```
0.0.0.0/0, <Inetinfo.exe><regist.exe>$, FILE_WRITE,  
C:¥data¥client.db; ALLOW
```

【 0 2 4 3 】

1 2 . 4 . 3) 動作例 2

具体的な動作の別の例として、外部ネットワーク 3 上のクライアント (1 3 3 . 2 0 1 . 5 7 . 2) から、内部ネットワーク 4 上の WWW サーバに対する不審アクセスがあって、それが攻撃である場合を示す。

【 0 2 4 4 】

このとき、第 1 ～ 第 1 0 実施形態のいずれかのファイアウォール装置によって、前記不審アクセスはおとり装置 3 7 に誘導され、偽サービス処理が行われる。

【 0 2 4 5 】

その後、おとり装置 3 7 のプロセッサ 2 0 1 上の WWW サーバでは、前記不審アクセスを受信を初めとして、以下のような処理を行う。

(A) 1 3 3 . 2 0 1 . 5 7 . 2 からのアクセスを受信する。

(B) 子プロセスを生成する。

(C) 子プロセスで、当該アクセスにおける不正な要求データに応じて、所定の処理を行う。例えば、

(C-1) コンテンツ領域に対する不正ファイル書き出し

(C-2) データベースに対する不正アクセス

などを行う。

【 0 2 4 6 】

上記 (A)、(B) は前記動作例 1 と同様であるため、ここでは攻撃時の動作 (C-1)、(C-2) のみについて具体例を示す。

【 0 2 4 7 】

1 2 . 4 . 3 . 1) コンテンツ領域に対する不正ファイル書き出し

WWW サーバまたはそのサブシステム (登録 CGI ・ 出力 CGI) などに脆弱性が存在するものとする。今、登録 CGI に脆弱性が存在し、「GET/cgi-bin/register.exe?path=C:\Inetpub\wwwroot\default.htm&data=abcd」というアクセスがあった場合に、コンテンツ領域内のファイル「C:\Inetpub\wwwroot\default.htm」に対して、データ「abcd」が書き込まれるものとする。

【 0 2 4 8 】

前記不正アクセスがあった場合、前記動作（C-1）が行われ、プロセッサ 2 0 1 はイベント 4 9 0 1（図 4 8 参照）をイベント管理部 3 7 0 1 に伝達する。イベント 4 9 0 1 の内容には、少なくとも、イベント名「FILE_WRITE」と、実行形ファイルのパス名「C:\Inetpub\wwwroot\default.htm」と、当該イベント発生源である前記孫プロセスのプロセス ID（8 0 1）とが記載される。

【0 2 4 9】

次に、イベント管理部 3 7 0 1 は、イベント 4 9 0 1 のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント 4 9 0 1 を追加する（図 4 8 参照）。その後、イベント 4 0 0 1 からイベント 4 9 0 1 への順方向リンクと、イベント 4 9 0 1 からイベント 4 0 0 1 への逆方向リンクを付加し、イベント 4 9 0 1 に関するイベントーコンテキスト対を攻撃検知部 3 7 0 2 に伝達する。

【0 2 5 0】

そして、攻撃検知部 3 7 0 2 は、イベント 4 9 0 1 に関するイベントーコンテキスト対に対して DT 判定を行う。その結果、イベント 4 9 0 1 のタイプを「<inetinfo.exe><inetinfo.exe><regist.exe>」、ドメインを「1 3 3 . 2 0 1 . 5 7 . 2」と判定する。

【0 2 5 1】

次に、攻撃検知部 3 7 0 2 は、DT 定義との照合を行う。本例の場合、以下のルール（図 3 9 のルール 6）に合致するので、その判定値「DENY」を採用し、攻撃があったものと判定する。

【0 2 5 2】

0.0.0.0/0, <inetinfo.exe>, FILE_WRITE, .*; DENY

そして、攻撃検知部 3 7 0 2 は、攻撃元ホスト「1 3 3 . 2 0 1 . 5 7 . 2」を含むアラームを直ちに生成して、前記ファイアウォール装置 1 へ送信する。

【0 2 5 3】

なお、WWWサーバもしくはそのサブシステムの脆弱性を介した不正なファイル書き込みがあった場合、すべて前記と同様にして攻撃であると判定される。

【0 2 5 4】

また、WWWサーバ以外のサーバ、例えばFTPサーバを介したコンテンツ領域への書き込みがあった場合、以下のルール（図39のルール5）に合致しない限り、すなわち、管理ドメインからの正当な保守作業でない限り、

10.56.192.0/24, ^<ftpd.exe>+\$, FILE_WRITE, C:¥Inetpub¥wwwroot¥.*; ALLOW

以下のルール（図39のルール8）により、攻撃であると判定される。

【0255】

0.0.0.0/0, .*, FILE_WRITE, C:¥Inetpub¥wwwroot¥.*; DENY

【0256】

12.4.3.2) データベースへの不正アクセス

WWWサーバまたはそのサブシステム（登録CGI・出力CGI）などに脆弱性が存在するものとし、「GET /cgi-bin/..%c1%c9../data/client.db HTTP/1.0」というアクセスによって、前記顧客データベースを窃取されるものとする。

【0257】

前記不正アクセスがあった場合、前記動作が行われたのを受けて、プロセッサ201はイベント5001（図49参照）をイベント管理部3701に伝達する。イベント5001の内容には、少なくとも、イベント名「FILE_READ」と、実行形ファイルのパス名「C:¥data¥client.db」と、当該イベント発生源である前記子プロセスのプロセスID（800）とが記載される。

【0258】

次に、イベント管理部3701は、イベント5001のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント5001を追加する。その後、イベント3801からイベント5001への順方向リンクと、イベント5001からイベント3801への逆方向リンクを付加し、イベント5001に関するイベントーコンテキスト対を攻撃検知部3702に伝達する。

【0259】

そして、攻撃検知部3702は、イベント5001のイベントーコンテキスト対に対してDT判定を行う。その結果、イベント5001のタイプを「<inetinfo.exe><inetinfo.exe>」、ドメインを「133.201.57.2」と判定する

。

【0260】

次に、攻撃検知部 3702 は、DT 定義との照合を行う。本例の場合、以下のルール（図 39 のルール 7）に合致するので、その判定値「DENY」を採用し、攻撃があったものと判定する。

【0261】

0.0.0.0/0, .*, FILE_READ|FILE_WRITE, C:¥data¥.*; DENY

そして、攻撃検知部 3702 は、攻撃元ホスト「133.201.57.2」を含むアラームを直ちに生成して、前記ファイアウォール装置 1 へ送信する。

【0262】

（第 13 実施形態）

13. 1）構成

図 50 は、本発明の第 13 実施形態におけるファイアウォール装置のブロック図である。本実施形態におけるファイアウォール装置 51 は、第 2 実施形態におけるファイアウォール装置 5 の誘導部 503 および信頼度管理部 502 に代えて、仮想サーバ部 5101 および信頼度管理部 5102 を備える。

【0263】

図 51 を参照すると、仮想サーバ部 5101 は、接続管理部 5201 と、第 1 入力バッファ 5202 および第 1 出力バッファ 5203 と、第 2 入力バッファ 5204 および第 2 出力バッファ 5205 とを有する。

【0264】

接続管理部 5201 は、パケットフィルタ 101 から伝達された各アクセスに含まれる要求データを信頼度管理部 5102 に入力し、その信頼度を取得する。また、その信頼度に応じて、第 1 入力バッファ 5202 または第 2 入力バッファ 5204 への要求データ転送処理や、第 1 出力バッファ 5203 または第 2 出力バッファ 5205 からの応答データ読み取り処理などを行う。

【0265】

第 1 入力バッファ 5202 および第 1 出力バッファ 5203 は、第 1 の内部通信インターフェース 104 を内部ネットワーク 4 に接続されており、それぞれサ

サーバ装置への要求データと、サーバ装置からの応答データを一時格納する。

【0266】

第2入力バッファ5204および第2出力バッファ5205は、おとり装置2に接続されており、それぞれおとり装置2への要求データと、おとり装置2からの応答データを一時格納する。また、信頼度管理部5102は、仮想サーバ部5101の接続管理部5201からの要求データ入力に応じて、その信頼度を出力する。

【0267】

13. 2) 動作

図52は、第13実施形態におけるファイアウォール装置33のフローチャートである。

【0268】

13. 2. 1) 仮接続

図52において、まず、ファイアウォール装置33がインターネット3上のあるホストから新たな接続を要求する入力IPパケットを受信して、第2実施形態におけるファイアウォール装置5と同様に、パケットフィルタ101とアクセス制御リスト管理部102とによって、その通過を認められた場合には、仮想サーバ5101の接続管理部5101は、前記ホストとの間に仮の接続を確立する（ステップG1）。

【0269】

13. 2. 2) 要求データの一時格納

その後、前記インターネット3上のホストから内部ネットワーク4上のサーバに対する要求データを受信する（ステップG2）。そして、接続管理部5201は、当該要求データを第1入力バッファ5202と第2入力バッファ5204とに伝達して、一時格納する（ステップG3）。

【0270】

13. 2. 3) 信頼度判定

そして、前記要求データを信頼度管理部5102に入力し、その信頼度cを取得し（ステップG4）、所定の閾値Tと比較を行う（ステップG5）。

【0271】

信頼度管理部 5102 における信頼度の計算方法としては、例えば、要求データをバイトデータの系列パターンとみなして、統計的なパターン解析によって、「頻繁に見られる要求データ」との類似度を計算し、当該類似度をもって信頼度 c とする方法がある。

【0272】

また、単に図 53 に示すような、過去に入力された要求データと信頼度との組を管理するためのテーブルを保持し、新たな要求データの入力があるたびに、当該テーブルを参照して、信頼度を求める方法を用いてもよい。より具体的には、ステップ G8-2 でおとり装置 2 によって正常であることが確認された場合にのみ信頼度を 1 とし、それ以外の場合、特にステップ G8-3 において、攻撃であることが確認された場合には、信頼度を 0 とし、以降この信頼度を再利用する方法を用いてもよい。

【0273】

さらに、前記テーブルに要求データを直接格納するのではなく、要求データの一方方向性ハッシュ関数値を格納する方法を用いてもよい。この場合、既知の要求データが再度入力された場合、その一方方向性ハッシュ関数値としても一致するため、その信頼度を正しく取得できる。さらに、要求データのサイズが非常に大きなものになり得る場合でも、一方方向性ハッシュ関数値は常に一定のサイズであるため、メモリ効率が良い。ただし、異なる要求データに対する一方方向性ハッシュ関数値が一致する（＝衝突する）場合があるが、一般に一方方向性ハッシュ関数値が一致する異なる 2 つの要求データ（特に、一方が正常でもう一方が攻撃であるような場合）を見つけることは困難とされるので、実用上の危険性は極めて小さい。

【0274】

13. 2. 3. 1) 要求データを信頼した場合

もし、 $c \geq T$ であれば（ステップ G5 の Y）、前記要求データを信頼できるものと判定し、第 1 入力バッファ 5202 と、第 2 入力バッファ 5204 とに、要求データの転送を指示する（ステップ G6-1）。この指示を受けた第 1 入力バ

ッファ 5202 は、直ちに格納済み要求データを、第 1 の内部通信インターフェース 104 を介して、内部ネットワーク 4 上のサーバに転送する。同様に、第 2 入力バッファ 5104 は、格納済み要求データを、第 2 の内部通信インターフェース 105 を介して、おとり装置 2 に転送する。

【0275】

13. 2. 3. 2) 応答データの確認

その後、第 1 の内部通信インターフェース 104 を介して、内部ネットワーク 4 上のサーバから応答データを受信したとき、第 1 出力バッファ 5203 は当該応答データを一時格納し、接続管理部 5201 に応答のあった旨を伝える（ステップ G7-1）。

【0276】

13. 2. 3. 3) 応答データの転送

接続管理部 5201 は、第 1 出力バッファ 5203 からデータ受信を伝達された後、直ちに前記ホストに向けて、第 1 出力バッファ 5203 に格納された応答データを転送する（ステップ G8-1）。

【0277】

13. 2. 4) 要求データを不審とした場合

一方、ステップ G5 の後、 $c < T$ であれば（ステップ G5 の N）、前記要求データを不審であると判定し、第 2 入力バッファ 5204 のみに、要求データの転送を指示する（ステップ G6-2）。第 2 入力バッファ 5204 は、この指示を受けて、直ちに第 2 の内部通信インターフェース 105 を介して、おとり装置 2 へ前記要求データを転送する。

【0278】

13. 2. 4. 1) 攻撃検知

そして、おとり装置 2 は第 2 実施形態と同様にして、攻撃の有無を判定する（ステップ G7-2）。

【0279】

13. 2. 4. 2) 攻撃が検知された場合

攻撃があった場合には（ステップ G7-2 の Y）、その旨を伝えるアラームを

生成して、ファイアウォール装置 5 1 へ送信する。制御インタフェース 1 0 6 を介して、当該アラームを受信したファイアウォール装置 3 3 は、第 2 実施形態におけるファイアウォール装置 5 と同様に、防御ルール判定部 1 0 7 から、信頼度管理部 5 1 0 2 に前記ホストから攻撃のあったことを伝達すると共に、アクセス制御リスト管理部 1 0 2 にアクセス制御ルールの更新を指示して、前記接続を遮断する（ステップ G 8 - 3）。

【0 2 8 0】

1 3 . 2 . 4 . 3) 攻撃が検知されなかった場合

一方、所定のタイムアウト時間内に攻撃が検知されなかった場合には（ステップ G 7 - 2 の N）、信頼度管理部 5 1 0 2 は接続管理部 5 2 0 1 へアラームを伝達する。接続管理部 5 2 0 1 は、当該アラームを受けて、第 1 入力バッファ 5 2 0 2 へ格納済み要求データの転送を指示する（ステップ G 8 - 2）。

【0 2 8 1】

なお、前記タイムアウト時間は、5 0 0 ミリ秒程度の時間を設定すれば通常十分であるが、入力 I P パケットがファイアウォール装置 5 1 に到達する時間間隔の平均値などをもって、適応的に変化させるようにしてもよい。

【0 2 8 2】

その後、第 1 の内部通信インターフェース 1 0 4 を介して、内部ネットワーク 4 上のサーバから応答データを受信したとき、第 1 出力バッファ 5 2 0 3 は当該応答データを一時格納し、接続管理部 5 2 0 1 に応答のあった旨を伝える（ステップ G 7 - 1）。

【0 2 8 3】

接続管理部 5 2 0 1 は、第 1 出力バッファ 5 2 0 3 からデータ受信を伝達された後、直ちに前記ホストに向けて、第 1 出力バッファ 5 2 0 3 に格納された応答データを転送する（ステップ G 8 - 1）。

【0 2 8 4】

1 3 . 3) 効果

第 1 3 実施形態におけるファイアウォール装置 5 1 によれば、1 回の接続について、複数の要求データ $r(1)$, $r(2)$, ..., $r(n)$ があって、その途中のある要求

データ $r(i)$ が不審とされるような場合、おとり装置 2 で当該要求データ $r(i)$ に対するサーバ動作から攻撃が検知されなかったとき、 $r(i)$ は内部ネットワーク 4 上の正規サーバへ必ず転送されるので、 $r(1) \sim r(n)$ の全要求データが正しい順序で正規サーバに到達することを保証できる。

【0285】

一方、おとり装置 2 で攻撃が検知されたとき、直ちに前記接続が遮断されるので、前記要求データ $r(i)$ を含め、それ以降の要求データは一切、前記正規サーバに到達しないことを保証できる。

【0286】

こうした性質は、データベースと連携する WWWサーバ（いわゆる「3 層システム」）や、Telnetサーバや、FTPサーバなどと、それぞれのクライアントとの間で行われるように、1 回の接続につき、複数の要求と応答が繰り返されるようなプロトコル（＝ステートフルプロトコル）に従うサービスの保護に適する。

【0287】

こうしたサービスにおいては、要求データ系列の順序が異なると、正しいサービス提供が保証できない。また、前記のように、攻撃用データを要求データ系列の一部として含むような場合にも、それまでの要求データ系列の順序が異なると、当該攻撃用データによるサーバの異常動作が観測できない場合がある。

【0288】

したがって、本実施形態におけるファイアウォール装置 50 とおとり装置 2 との組み合わせによる攻撃防御システムは、ステートフルプロトコルに従うサービスについて、その正常動作および異常動作を誤りなく判定し、攻撃を確実に防御することができる。

【0289】

また、WWWサーバによる静的コンテンツ提供のような、ステートレスプロトコルを対象とする場合でも、本実施例による誘導方法によれば、インターネット 3 上のホストに転送される応答データは常に正規サーバの出力する応答データである。したがって、静的コンテンツの改ざんなどがおとり装置 2 で発生していた場

合でも、改ざんされたコンテンツが前記ホストに到達することが一切なく、常に正しいコンテンツの提供が保証できる。

【0290】

13.4) 具体例

13.4.1) 構成

図54を参照すると、本実施例は、インターネット3上のFTPクライアント302と、内部ネットワーク4上のFTPサーバ402と、ファイアウォール装置51と、おとり装置2とから構成される。

【0291】

FTPクライアント302は、FTPサーバ402に向けていくつかの要求データを送信するが、それらは全て、ファイアウォール装置51で中継される。また、ファイアウォール装置51は、FTPクライアント302から入力される要求データをおとり装置2へも転送する。さらに、おとり装置2のプロセッサ201上では、FTPサーバ402と同じFTPサービスが提供されている。

【0292】

13.4.2) 動作

FTPクライアント302は、FTPサーバ402に向けて、要求データを順次送信するが、本実施例では、FTPクライアント302が、

1) 匿名ログイン

2) ファイルアップロード

を行う場合の、ファイアウォール装置51の動作例を示す。

【0293】

また、FTPサーバ402とおとり装置2とは、非常に長いファイル名を処理したときにバッファオーバーフローを起こして、シェルが不正に操作される、という共通の脆弱性をもつものとする。

【0294】

さらに、おとり装置2の攻撃検知部202には、プロセッサ201で動作するFTPサーバがシェルを起動することを禁止するような正常動作定義がなされているものとする。

【0 2 9 5】

1 3 . 4 . 2 . 1) 仮接続

まず、F T Pクライアント 3 0 2 は、F T Pサーバ 4 0 2 へのログインに先立って、所定のT C P接続を確立するため、F T Pサーバ 4 0 2 に向けてS Y Nパケットを送信する。

【0 2 9 6】

当該S Y Nパケットが、ファイアウォール装置 5 1 に到達したとき、ファイアウォール装置 5 1 の仮想サーバ 5 1 0 1 は、F T Pサーバ 4 0 2 に代わって、前記S Y Nパケットに対応するS Y N - A C Kパケットを応答する。

【0 2 9 7】

その後、F T Pクライアント 3 0 2 は、さらにA C KパケットをF T Pサーバ 4 0 2 へ向けて送信する。当該A C Kパケットがファイアウォール装置 5 1 に到達したとき、仮想サーバ 5 1 0 1 は、新たなT C P接続が確立したものと判定する。

【0 2 9 8】

そして、仮想サーバ 5 1 0 1 の接続管理部 5 2 0 1 は、F T Pサーバ 4 0 2 と、おとり装置 2 とに対して、F T Pクライアント 3 0 2 に代わって、個別にT C P接続を確立する。

【0 2 9 9】

1 3 . 4 . 2 . 2) 匿名ログイン

次に、F T Pクライアント 3 0 2 は、F T Pサーバ 4 0 2 へ向けて、匿名ログインを行うための要求データを送信する。

【0 3 0 0】

一般に、F T Pサーバに対する匿名ログインは、以下のような 2 個の要求データを送信する。

- ・第 1 の要求データ (r1) : ユーザ名を示すものであり、一般に「anonymous」である。
- ・第 2 の要求データ (r2) : パスワードを示すものであり、一般に「user@domain」の形式をもつメールアドレスである。

【0301】

r1が、ファイアウォール装置51に到達したとき、仮想サーバ5101の接続管理部5201は、まず、r1を第1入力バッファ5202と、第2入力バッファ5204とに伝達し、一時格納する。

【0302】

その後、r1を信頼度管理部5102に入力し、その信頼度を取得する。このとき、信頼度管理部5102は、例えば、図53のような信頼度管理テーブルに対して、r1をキーとして信頼度を検索する。このとき、r1のエントリがあれば、その信頼度clを、接続管理部5201に出力する。もし、r1のエントリが無ければ、信頼度の初期値「0」をもつ、新たなエントリを追加し（図55の網掛け部）、信頼度0を接続管理部5201に出力する。本実施例では、すでにr1のエントリが存在し、その信頼度が「1」であるものとする。

【0303】

そして、接続管理部5201は、所定の閾値と前記信頼度を比較する。本実施例では、閾値を1とする。したがって、接続管理部5201は、r1を信頼し、第1入力バッファ5202と、第2入力バッファ5204とに、r1の転送を指示する。

【0304】

転送を指示された第1入力バッファ5202および第2入力バッファ5204は、それぞれ、FTPサーバ402およびおとり装置2へ、r1を転送する。

【0305】

その後、r1を受信したFTPサーバ402は、パスワードの入力を求める応答データs1をFTPクライアント302へ向けて送信する。s1がファイアウォール装置51に到達したとき、s1は一旦第1出力バッファ5203に格納される。そして、第1出力バッファ5203は、新たな応答データを受信した旨を、接続管理部5201に伝達する。

【0306】

そして、接続管理部5201は、第1出力バッファ5203に格納されたs1を、FTPクライアント302に向けて転送する。なお、おとり装置2からもs1が

送信され、第2出力バッファ 5 2 0 5 が s1 を格納し、接続管理部 5 2 0 1 に応答データ受信を伝達するが、本実施例における接続管理部 5 2 0 1 は、これを無視する。

【0 3 0 7】

以上のようにして、FTPクライアント 3 0 2 からFTPサーバ 4 0 2 へ向けて送信された要求データ r1 は、適切にFTPサーバ 4 0 2 およびおとり装置 2 へ転送される。

【0 3 0 8】

次に、パスワード入力である要求データ r2 についても、信頼度管理部 5 1 0 2 は、その信頼度を「1」と出力するものとする。したがって、r2 は r1 と同様にし、FTPサーバ 4 0 2 およびおとり装置 2 へ転送される。こうして、FTPクライアント 3 0 2 は、FTPサーバ 4 0 2 およびおとり装置 2 の双方に対して、匿名ログインを完了することができる。

【0 3 0 9】

1 3 . 4 . 2 . 3) ファイルアップロード

匿名ログインを完了したFTPクライアント 3 0 2 は、ファイルアップロードを行う。FTPサービスにおけるファイルアップロードは、以下の形式のコマンドを要求データに含めることで行われる。

【0 3 1 0】

「PUT <ファイル名>」。

【0 3 1 1】

ここで、以下の2種類の要求データを考える。

(A) r 3 - 1 : 「PUT FILE. TXT」

(B) r 3 - 2 : 「PUT XXXXXXXXX . . . <シェルコード>」。

【0 3 1 2】

r 3 - 1 は、「FILE. TXT」という名前のファイルをFTPサーバ 4 0 2 にアップロードしようとするものであり、正常な要求データであるとする。一方 r 3 - 2 は、FTPサーバ 4 0 2 にバッファオーバーフローを引き起こさせて、ファイル名の一部として含められたシェルコードを不正にFTPサーバ 4 0 2

内のシェルに実行させようとするものであるとする。

【0313】

13. 4. 2. 3. 1) r3-1が入力された場合

まず、FTPクライアント302から要求データr3-1が送信された場合を示す。

【0314】

r3-1がファイアウォール装置51に到達した際、前記r1と同様にして、接続管理部5201によって、第1入力バッファ5202および第2入力バッファ5204とに格納され、r3-1が信頼度管理部5102に入力される。

【0315】

信頼度管理部5102は、前記信頼度管理テーブルを参照するが、このとき、r3-1のエントリがないものとする。この場合、信頼度管理部5102は、信頼度管理テーブルに、r3-1のエントリを新たに追加する。また、r3-1の信頼度として、所定の初期値「0」を設定し、「0」を接続管理部5201に出力する。

【0316】

接続管理部5201は、r3-1の信頼度「0」を取得したのち、閾値「1」との比較を行って、閾値より小さな信頼度であることを確認し、r3-1を不審とみなす。そして、第2入力バッファ5204のみに、r3-1の転送を指示する。

【0317】

第2入力バッファ5204は、前記転送指示を受けて、おとり装置2にr3-1を転送する。

【0318】

おとり装置2は、r3-1を受信して、ファイル「FILE.TXT」を保存した後、保存が完了した旨を伝える応答データs3-1を送信する。

【0319】

その後、応答データs3-1は、ファイアウォール装置51に到達し、第2出力バッファ5205に格納され、第2出力バッファ5205は、その旨を接続管

理部 5201 に通知する。そして、接続管理部 5201 は、信頼度管理部 5102 に r3-1 が正常であることを通知し、信頼度管理部 5102 は、前記信頼度管理テーブルを更新して、r3-1 の信頼度を「1」にする。

【0320】

さらに、接続管理部 5201 は、第1入力バッファ 5202 に r3-1 の転送を指示して、第1入力バッファ 5202 に r3-1 を FTP サーバ 402 に転送させる。

【0321】

その後、FTP サーバ 402 は、ファイル「FILE. TXT」を保存し、その完了を伝える応答データ s3-1 を送信する。

【0322】

FTP サーバ 402 からの応答データ s3-1 は、第1出力バッファ 5203 に格納され、第1出力バッファ 5203 は、その旨を接続管理部 5201 に通知する。そして、接続管理部 5201 は、s3-1 を FTP クライアント 302 に転送する（図56参照）。

【0323】

以上のようにして、FTP クライアント 302 から送信されたファイル「FILE. TXT」は、FTP サーバ 402 およびおとり装置 2 に適切に保存される。

【0324】

13. 4. 2. 3. 2) r3-2 が入力された場合

次に、FTP クライアント 302 から不正な要求データ r3-2 が送信された場合を示す。

【0325】

r3-2 がファイアウォール装置 51 に到達した際、前記 r3-1 と同様にし、接続管理部 5201 によって、第1入力バッファ 5202 および第2入力バッファ 5204 とに格納され、r3-2 が信頼度管理部 5102 に入力される。

【0326】

信頼度管理部 5102 は、前記信頼度管理テーブルを参照するが、このとき、

やはり、r 3-2 のエントリがないものとする。この場合、信頼度管理部 5002 は、信頼度管理テーブルに、r 3-1 のエントリを新たに追加する。また、r 3-2 の信頼度として、所定の初期値「0」を設定し、「0」を接続管理部 5201 に出力する。

【0327】

接続管理部 5201 は、r 3-2 の信頼度「0」を取得したのち、閾値「1」との比較を行って、閾値より小さな信頼度であることを確認し、r 3-2 を不審とみなす。

【0328】

そして、第2入力バッファ 5204 のみに、r 3-2 の転送を指示する。第2入力バッファ 5204 は、前記転送指示を受けて、おとり装置 2 に r 3-2 を転送する。

【0329】

おとり装置 2 が r 3-2 を受信すると、プロセッサ 201 上で、(偽の) FTP サーバはバッファオーバーフローによってシェルを起動し、r 3-2 に含まれる不正なシェルコードを実行しようとする。おとり装置 2 の攻撃検知部 202 は、当該シェル起動を攻撃と検知し、直ちにアラームをファイアウォール装置 51 に送信する。

【0330】

前記アラームを受信したファイアウォール装置 51 は、まず、防御ルール判定部 107 と、アクセス制御リスト管理部 102 と、パケットフィルタ 101 とによって、第1実施形態におけるファイアウォール装置 1 と同様に、FTP クライアント 302 からの以降のアクセスを遮断する。また、防御ルール判定部 107 は、アラームの受信を接続管理部 5201 にも通知する。

【0331】

アラーム受信通知を受けた接続管理部 5201 は、ただちに FTP クライアント 302 との接続を遮断する。また、望ましくは、第1入力バッファ 5202 に格納された r 3-2 を消去する。

【0332】

以上のようにして、不正な要求データ r 3 - 2 は、到達するとしてもおとり装置 2 に限られ、FTP サーバ 4 0 2 に到達しない（図 5 7 参照）。

【0333】

（第 1 4 実施形態）

図 5 8 に示すように、内部ネットワーク 4 上のサーバ（例えば FTP サーバ 4 0 2）からおとり装置 2 へ少なくともファイルシステムの内容を複製するミラーリング装置 5 9 0 1 をさらに備えてもよい。

【0334】

おとり装置 2 で攻撃が検知されファイアウォール装置 5 1 の防御ルール判定部 1 0 7 にアラームが伝達された際、防御ルール判定部 1 0 7 は、さらにミラーリング装置 5 9 0 1 にもアラーム受信を通知する。

【0335】

当該通知を受けたミラーリング装置 5 9 0 1 は、前記内部ネットワーク 4 上のサーバのファイルシステム 4 0 2 1 を読み取り、その内容をおとり装置 2 上のファイルシステム 2 0 1 1 へ複製する。こうすることにより、おとり装置 2 上で不正なファイル書込みが発生しても、その被害をリアルタイムに復旧することができる。

【0336】

本実施形態ではファイルシステムを具体例として挙げたが、その他に、さらにメモリモジュールの内容を複製するようにしてメモリ内の異常を復旧するようにしてもよい。また、おとり装置 2 から送信されるアラームに、書換えられたファイルのパス名、あるいは、メモリ領域を記載するようにして、被害を受けた部分のみを複製できるようにしてもよい。

【0337】

（第 1 5 実施形態）

図 5 9 は、本発明の第 1 5 実施形態におけるファイアウォール装置の概略的構成図である。本実施形態におけるファイアウォール装置 6 3 は、第 1 3 実施形態におけるファイアウォール装置 5 2 の仮想サーバ 5 2 0 1 の前面に暗号処理部 6 3 0 1 を備える。

【0338】

暗号処理部 6301 は、パケットフィルタ 101 から得られた暗号化入力 IP パケットを復号した入力 IP パケットものを仮想サーバ 5201 に伝達し、仮想サーバ 5201 から得られた出力 IP パケットを暗号化した暗号化出力 IP パケットをパケットフィルタ 101 に伝達する。

【0339】

このようにすることで、インターネット 3 および内部ネットワーク 4 との間で暗号化通信が行われる場合にも、おとり装置への誘導を行うことができる。

【0340】

(第 16 実施形態)

上記第 1 ～ 第 15 実施形態では、誘導部（または仮想サーバ部）、防御ルール判定部、パケットフィルタ、および、アクセス制御リスト管理部が一つのユニットになったファイアウォール装置を例示したが、本発明はこれに限定されるものではない。

【0341】

たとえば、次のようにハードウェア的に 2 ユニットで構成し、それらをネットワークで接続することもできる。

- ・少なくともパケットフィルタおよびアクセス制御リスト管理部を有するファイアウォール装置
- ・少なくとも誘導部（または仮想サーバ部）および防御ルール判定部を有するスイッチ装置。

【0342】

従来のファイアウォール装置は、遠隔からアクセス制御リストの部分的更新を行う機能を有していることが多いので、既に設置済みのファイアウォール装置に加えて、上記スイッチ装置を設置することで、第 1 ～ 第 14 実施形態における 1 ユニットのファイアウォール装置と同等の機能を実現できるというメリットがある。

【0343】

図 60 は本発明の第 16 実施形態による攻撃防御システムの概略的構成図であ

る。本実施形態において、ファイアウォール装置 7001 にはパケットフィルタ 101 およびアクセス制御リスト管理部 102 が設けられ、スイッチ装置 7002 には誘導部 501、信頼度管理部 502 および防御ルール判定部 107 が設けられている。パケットフィルタ 101 と誘導部 501 との間、および、アクセス制御リスト管理部 102 と防御ルール判定部 107 との間をネットワークを介して接続することで、第 1 ～ 第 15 実施形態による攻撃防御システムを実現することができる。

【0344】

【発明の効果】

以上詳細に説明したように、本発明による攻撃防御システム及び方法によれば、IP パケットのヘッダ情報に基づいてパケットの誘導を行うために、外部ネットワークから内部ネットワークへのアクセスにおいて通信路暗号化技術が用いられた場合でも、攻撃を検知および防御することができる。いかなる通信路暗号化技術が用いられたとしても、少なくとも IP ヘッダに記載されたソース IP アドレスもしくはデスティネーション IP アドレスは暗号化されず、さらにファイアウォール装置によるおとり装置への誘導は、これら IP ヘッダに記載された情報を基に行うことができるためである。

【0345】

また、本発明によれば、ファイアウォール装置によるおとり装置への誘導方法が少ないパラメータを基にした簡易なアルゴリズムで実現できるため、高速ネットワーク環境においても、ネットワーク性能を高いレベルで維持できる。

【0346】

さらに、本発明によれば、おとり装置へ誘導されて攻撃が検出された全てのパケットについて、その送信元ホストからの以降のアクセスを拒否するように動的な防御を行うことで後続する攻撃を全てファイアウォール装置で防御することができる。このために内部ネットワークへの通信経路が無くなり、検出された攻撃用パケットが一切内部ネットワークに到達しない。

【図面の簡単な説明】

【図 1】

本発明による攻撃防御システムの概略的ブロック図である。

【図 2】

本発明の第 1 実施形態による攻撃防御システムのファイアウォール装置 1 およびおとり装置 2 の構成を示すブロック図である。

【図 3】

図 2 のファイアウォール装置 1 におけるアクセス制御リスト管理部 102 の模式的構成図である。

【図 4】

アクセス制御リストデータベース 1021 の内容を例示した模式図である。

【図 5】

誘導部 103 に設けられた誘導リストの一例を示す模式図である。

【図 6】

防御ルール判定部 107 に保持されているアクセス制御ルールのひな型を例示した模式図である。

【図 7】

本発明の第 1 実施形態による攻撃防御システムの動作を示すフローチャートである。

【図 8】

本発明の第 1 実施形態のファイアウォール装置でアドレス変換処理を行う際の好適な一例を示すブロック図である。

【図 9】

第 1 実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図 10】

第 1 実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図 11】

第 1 実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図 12】

おとり装置 2 における攻撃検知動作を説明するための模式図である。

【図 13】

第 1 実施形態におけるアクセス制御リストの更新動作例を説明するための模式図である。

【図 1 4】

第 1 実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図 1 5】

本発明の第 2 実施形態による攻撃防御システムのブロック図である。

【図 1 6】

本発明の第 2 実施形態による攻撃防御システムの動作を示すフローチャートである。

【図 1 7】

本実施形態における信頼度とパケット転送先の関係を示すグラフである。

【図 1 8】

(A) は、外れ値度計算を用いた信頼度管理部 5 0 2 の概略的構成図であり、
(B) は、その一例を示す詳細なブロック図である。

【図 1 9】

本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【図 2 0】

本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【図 2 1】

本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【図 2 2】

本発明の第 3 実施形態による攻撃防御システムのファイアウォール装置の概略的構成を示すブロック図である。

【図 2 3】

第 3 実施形態による攻撃防御システムのファイアウォール装置の一例を示す詳細なブロック図である。

【図 2 4】

本発明における第 4 実施形態による攻撃防御システムのファイアウォール装置の一例を示すブロック図である。

【図 2 5】

信頼度管理部 701 における信頼度参照処理を示すフローチャートである。

【図 2 6】

本発明の第 6 実施形態による攻撃防御システムのファイアウォール装置 9 を示す概略的ブロック図である。

【図 2 7】

本実施形態によるファイアウォール装置 9 の動作を示すフローチャートである。

【図 2 8】

本発明の第 7 実施形態による攻撃防御システムのファイアウォール装置 10 を示す概略的ブロック図である。

【図 2 9】

アクセス制御リスト管理部 1002 の管理動作を示すフローチャートである。

【図 3 0】

本発明の第 8 実施形態による攻撃防御システムの概略的構成図である。

【図 3 1】

本発明の第 10 実施形態による攻撃防御システムの概略的構成図である。

【図 3 2】

本発明の第 11 実施形態による攻撃防御ユニットの概略的構成図である。

【図 3 3】

本発明の第 12 実施形態におけるおとり装置の構成を示すブロック図である。

【図 3 4】

第 12 実施形態におけるおとり装置の全体的動作を示すフローチャートである。

【図 3 5】

第 12 実施形態において使用されるプロセス種別判定テーブルの一例を示す図

である。

【図 3 6】

イベント管理部におけるイベント管理キューの一例を示す図である。

【図 3 7】

第 1 2 実施形態におけるイベント管理部が行うリンク付け処理の 1 例を示すフローチャートである。

【図 3 8】

第 1 2 実施形態におけるイベント管理部が出力するイベントーコンテキスト対の概念図である。

【図 3 9】

ドメインタイプ制約つき正常動作定義（D T 定義）ファイルの一例を示す図である。

【図 4 0】

第 1 2 実施形態における攻撃検知部が解釈するドメインタイプ制約の概念図である。

【図 4 1】

第 1 2 実施形態におけるおとり装置のイベント管理部が行うネットワークイベント追加の具体例を示す模式図である。

【図 4 2】

第 1 2 実施形態におけるおとり装置のイベント管理部が行うプロセスイベント走査の具体例を示す模式図である。

【図 4 3】

第 1 2 実施形態におけるおとり装置のイベント管理部が行うリンク付けの具体例を示す模式図である。

【図 4 4】

第 1 2 実施形態におけるおとり装置のイベント管理部が行う子プロセス生成イベントの追加およびリンク付けの具体例を示す模式図である。

【図 4 5】

第 1 2 実施形態におけるおとり装置のイベント管理部が行う子プロセスが発生

させたファイルイベントの追加およびリンク付けの具体例を示す模式図である。

【図 4 6】

第 1 2 実施形態におけるおとり装置のイベント管理部が行う孫プロセス生成イベントの追加およびリンク付けの具体例を示す模式図である。

【図 4 7】

第 1 2 実施形態におけるおとり装置のイベント管理部が行う孫プロセスが発生させたファイルイベントの追加およびリンク付けの具体例を示す模式図である。

【図 4 8】

第 1 2 実施形態のおとり装置における攻撃発生時のイベント管理キュー状態を示す具体例を示す模式図である。

【図 4 9】

第 1 2 実施形態のおとり装置における攻撃発生時のイベント管理キュー状態を示す別の具体例を示す模式図である。

【図 5 0】

本発明の第 1 3 実施形態におけるファイアウォール装置の構成を示すブロック図である。

【図 5 1】

第 1 3 実施形態におけるファイアウォール装置の仮想サーバ部の詳細なブロック図である。

【図 5 2】

第 1 3 実施形態におけるファイアウォール装置の動作を示すフローチャートである。

【図 5 3】

第 1 3 実施形態におけるファイアウォール装置の信頼度管理部に格納される信頼度管理テーブルの一例を示す図である。

【図 5 4】

第 1 3 実施形態におけるファイアウォール装置の動作を説明するための攻撃防御システムの概略的ブロック図である。

【図 5 5】

第13実施形態における信頼度管理部が行う信頼度管理テーブルへの新規エントリ追加の具体例を示す図である。

【図56】

第13実施形態におけるファイアウォール装置が行う正常動作確認時の動作の具体例を示す図である。

【図57】

第13実施形態におけるファイアウォール装置が行う、攻撃検知時の動作の具体例を示す図である。

【図58】

本発明の第14実施形態による攻撃防御システムの概略的ブロック図である。

【図59】

本発明の第15実施形態におけるファイアウォール装置の概略的ブロック図である。

【図60】

本発明の第16実施形態による攻撃防御システムの概略的構成図である。

【符号の説明】

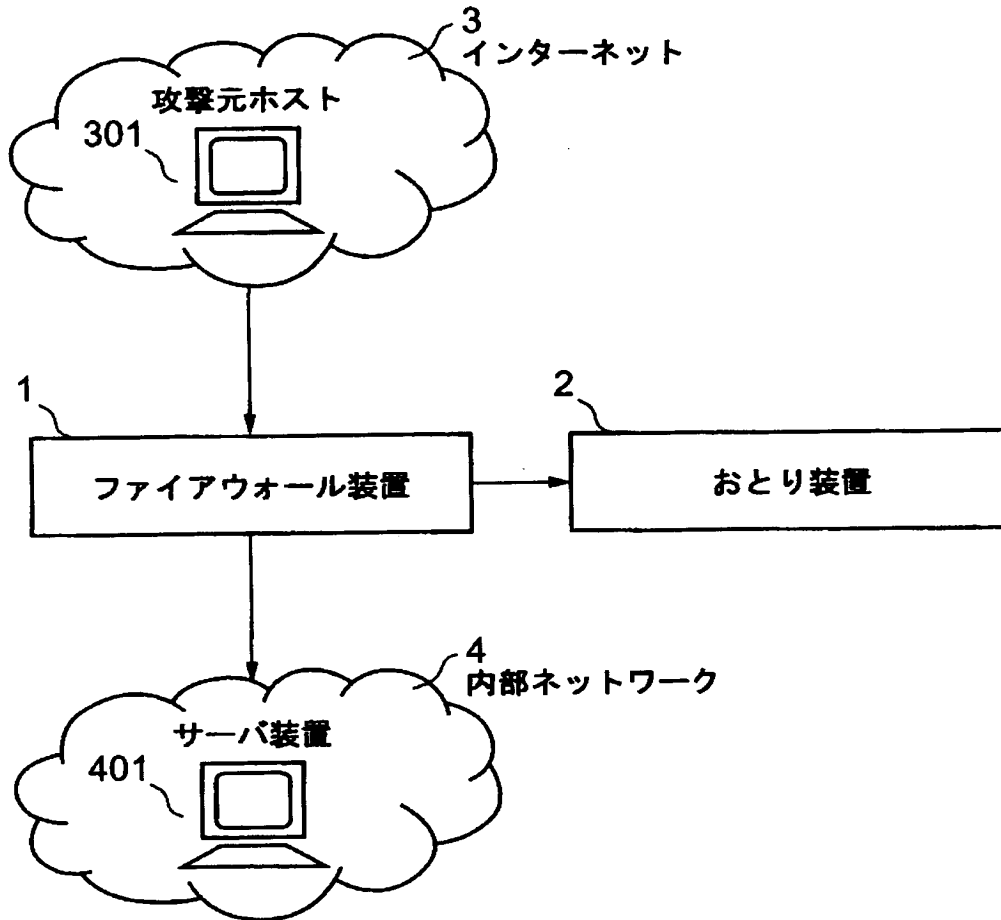
- 1 ファイアウォール装置
- 100 外部通信インタフェース
- 101 パケットフィルタ
- 102 第1のアクセス制御リスト管理部
- 1021 アクセス制御リストデータベース
- 1022 検索処理部
- 1023 更新処理部
- 103 誘導部
- 1031 アドレス変換部
- 104 第1の内部通信インタフェース
- 105 第2の内部通信インタフェース
- 106 制御インタフェース
- 107 防御ルール判定部

- 2 おとり装置
 - 201 プロセッサ
 - 2011 ファイルシステム
 - 202 攻撃検知部
- 3 インターネット
 - 301 攻撃元ホスト
 - 302 通常のホスト
- 4 内部ネットワーク
 - 401 サーバ装置
- 5 ファイアウォール装置
 - 501 誘導部
 - 502 信頼度管理部
 - 5021 外れ値検知部
- 6 ファイアウォール装置
- 7 ファイアウォール装置
 - 701 信頼度管理部
 - 7011 リアルタイム信頼度データベース
 - 7012 複製処理部
 - 7013 長期信頼度データベース
 - 7014 更新処理部
- 8 ファイアウォール装置
- 9 ファイアウォール装置
 - 901 誘導部
 - 9011 バッファ
 - 9012 ICMP監視部
- 10 ファイアウォール装置
 - 1001 防御ルール判定部
 - 1002 アクセス制御リスト管理部
- 21 おとりクラスタ

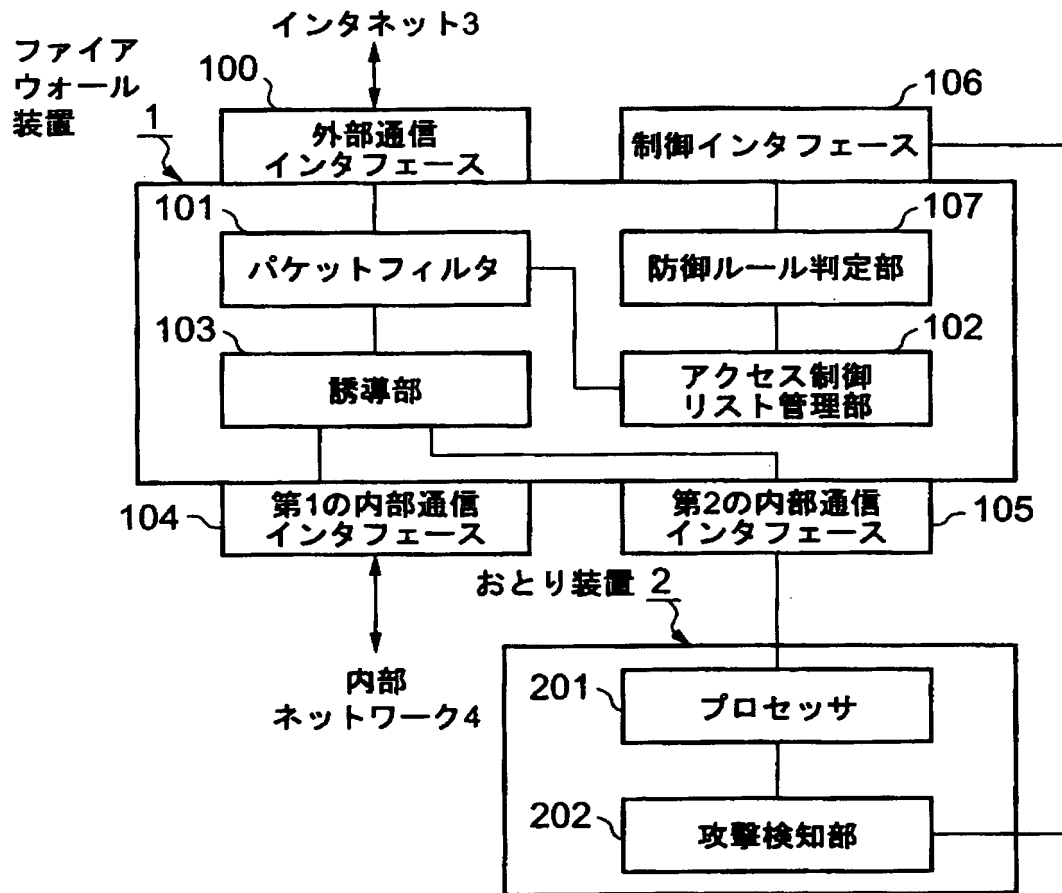
- 3 7 第 2 のおとり装置
 - 3 7 0 1 イベント管理部
 - 3 7 0 2 第 2 の攻撃検知部
- 4 1 0 1 ドメインタイプ制約つき正常動作定義ファイル
- 3 5 0 1 第 1 のイベント
- 3 6 0 1 第 2 のイベント
- 3 8 0 1 第 3 のイベント
- 3 9 0 1 第 4 のイベント
- 4 0 0 1 第 5 のイベント
- 4 1 0 1 第 6 のイベント
- 4 9 0 1 第 7 のイベント
- 5 0 0 1 第 8 のイベント
- 5 1 第 8 のファイアウォール装置
 - 5 1 0 1 仮想サーバ部
 - 5 1 0 2 第 3 の信頼度管理部
- 5 2 0 1 接続管理部
- 5 2 0 2 第 1 入力バッファ
- 5 2 0 3 第 1 出力バッファ
- 5 2 0 4 第 2 入力バッファ
- 5 2 0 5 第 2 出力バッファ
- 6 2 第 9 のファイアウォール装置
 - 6 2 0 1 暗号処理部
- 3 0 3 F T P クライアント
- 4 0 2 F T P サーバ
 - 4 0 2 1 ファイルシステム
- 6 9 0 1 ミラーリング装置
- 7 0 0 1 ファイアウォール装置
- 7 0 0 2 スイッチ装置

【書類名】 図面

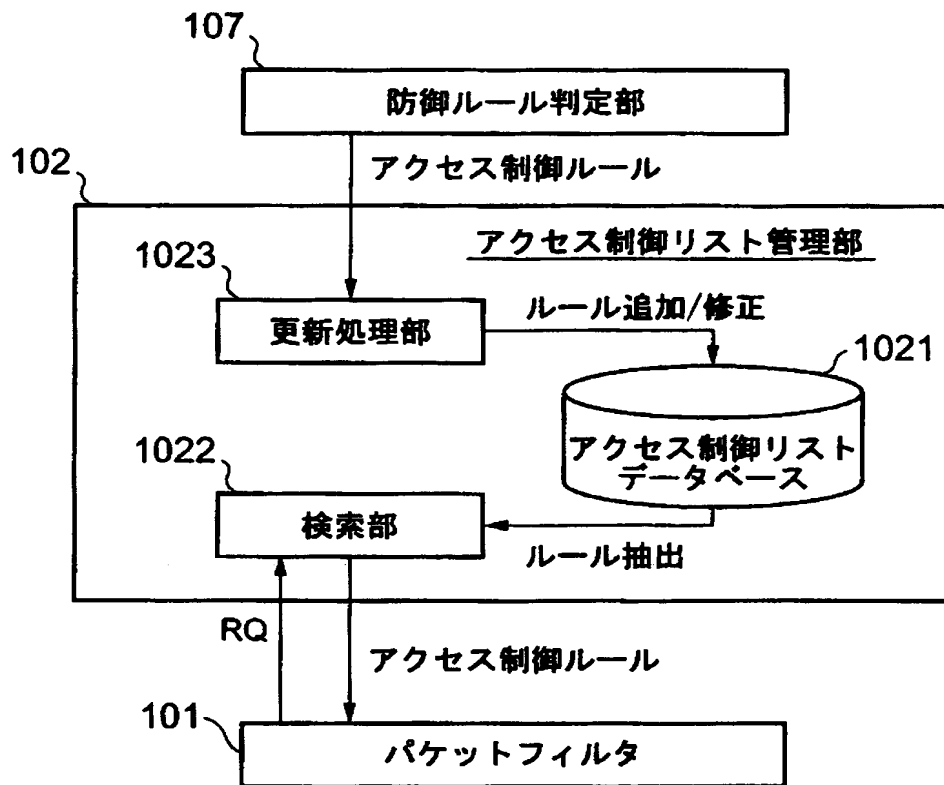
【図 1】



【図 2】



【図 3】



【図 4】

1021

アクセス制御リストデータベース		
ソースIPアドレス (SRC)	ディスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

*…任意のアドレスにマッチ

ACCEPT…パケットの受理

DENY…パケットの拒否(ICMPエラーを通知)

DROP…パケットの廃棄(ICMPエラーを通知しない)

【図 5】

誘導リスト

1.2.3.1
1.2.3.2
1.2.3.3
1.2.3.5
1.2.3.6
⋮

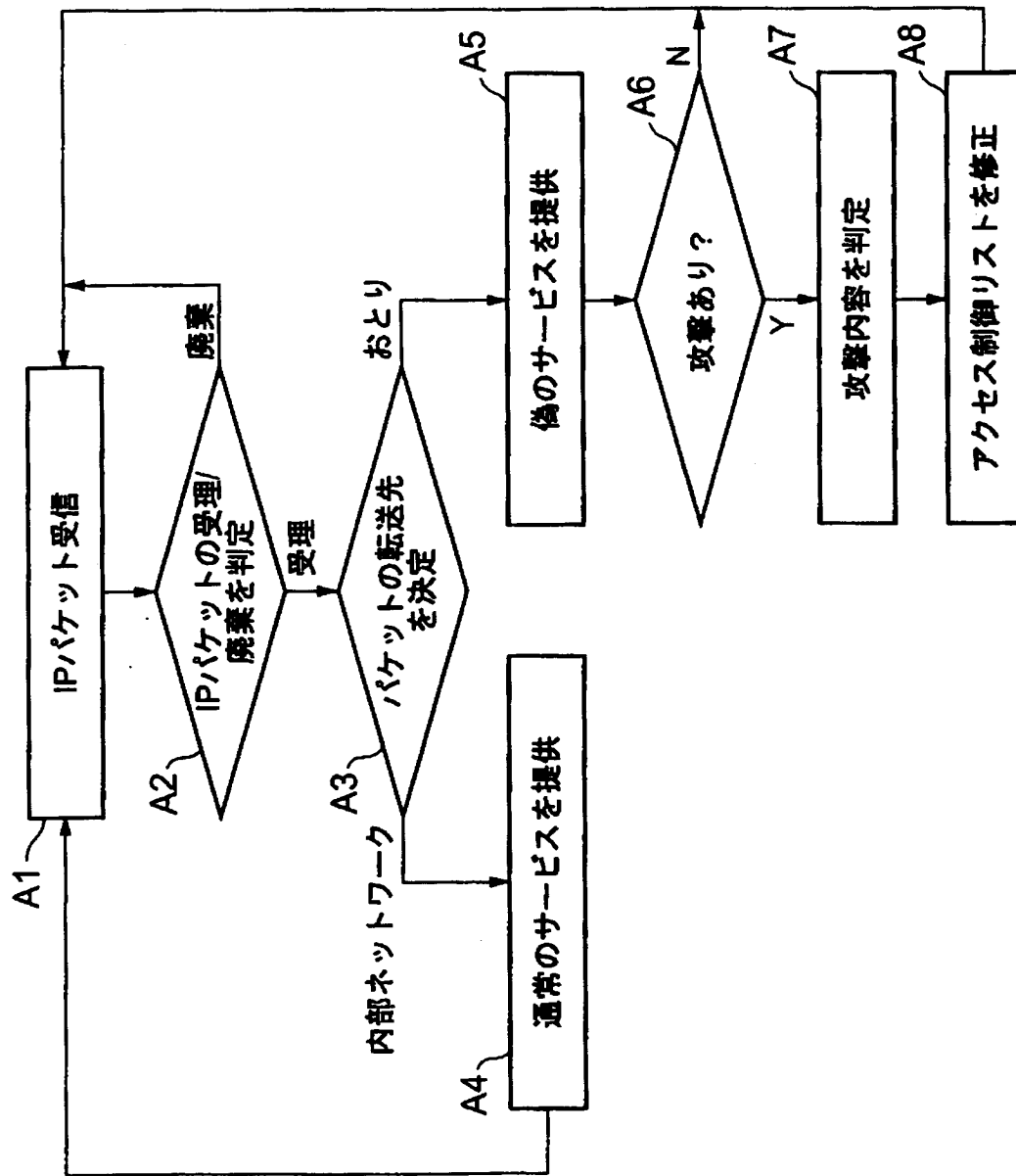
【図 6】

107 {

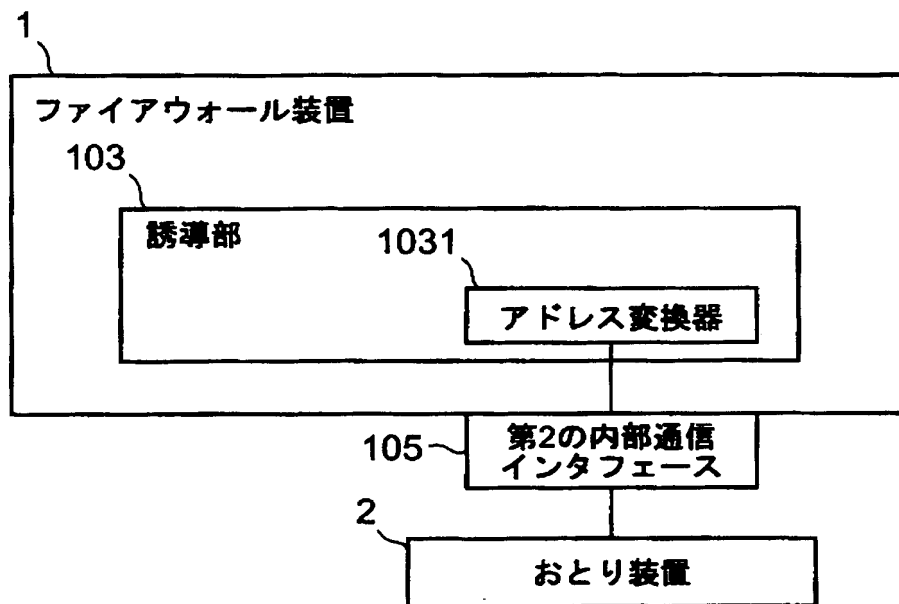
防御ルール判定部				
攻撃種別	ソースIPアドレス (SRC)	デスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)	
RECON	—	—	—	
INTRUSION	\${SRC_IP_ADDRESS}	*	DROP	
DESTRUCTION	\${SRC_IP_ADDRESS}	*	DROP	

—…無指定(何もしない)
\${}…置換用変数

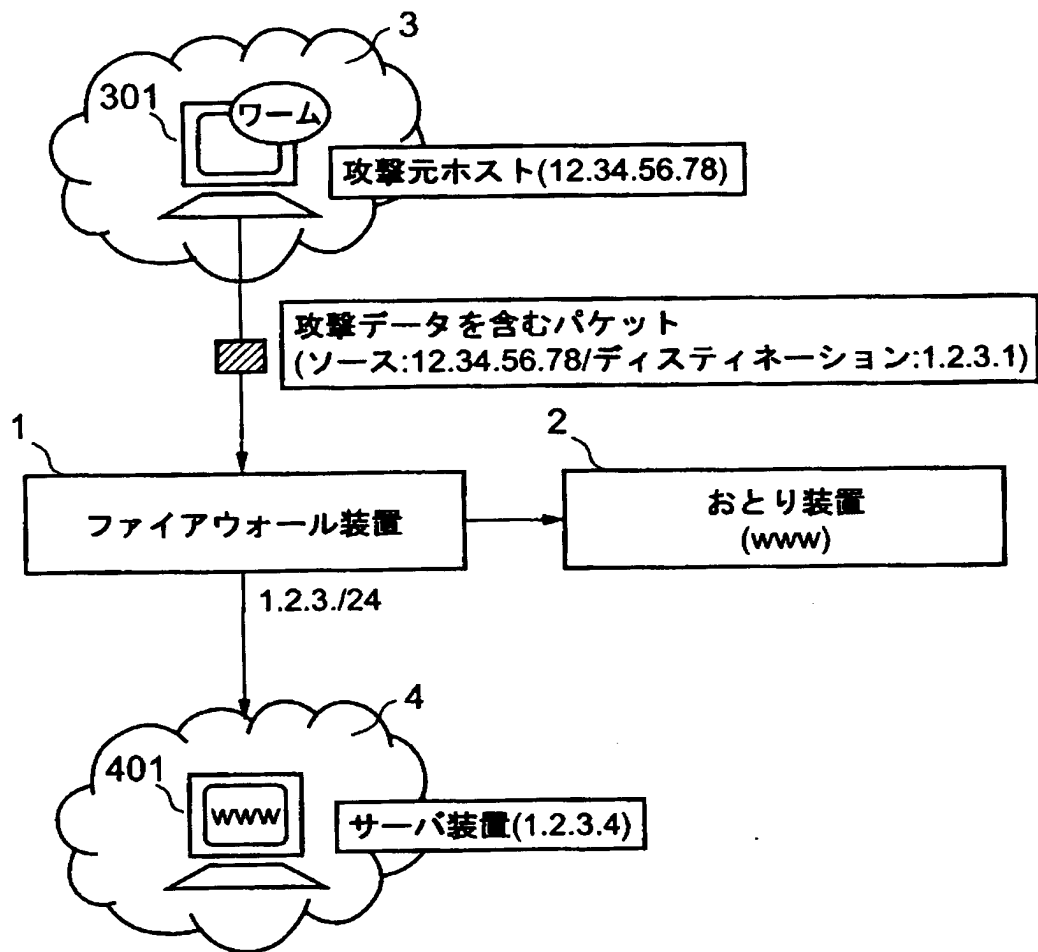
【図 7】



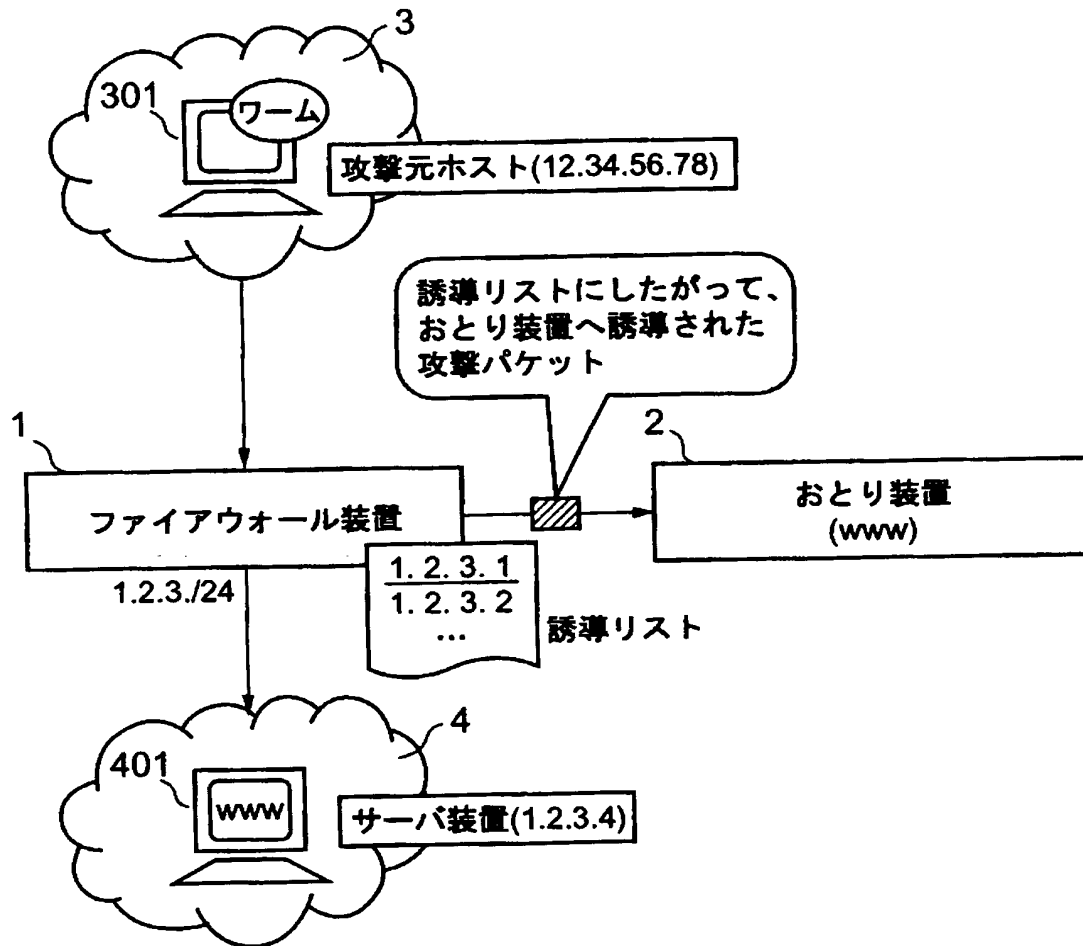
【図 8】



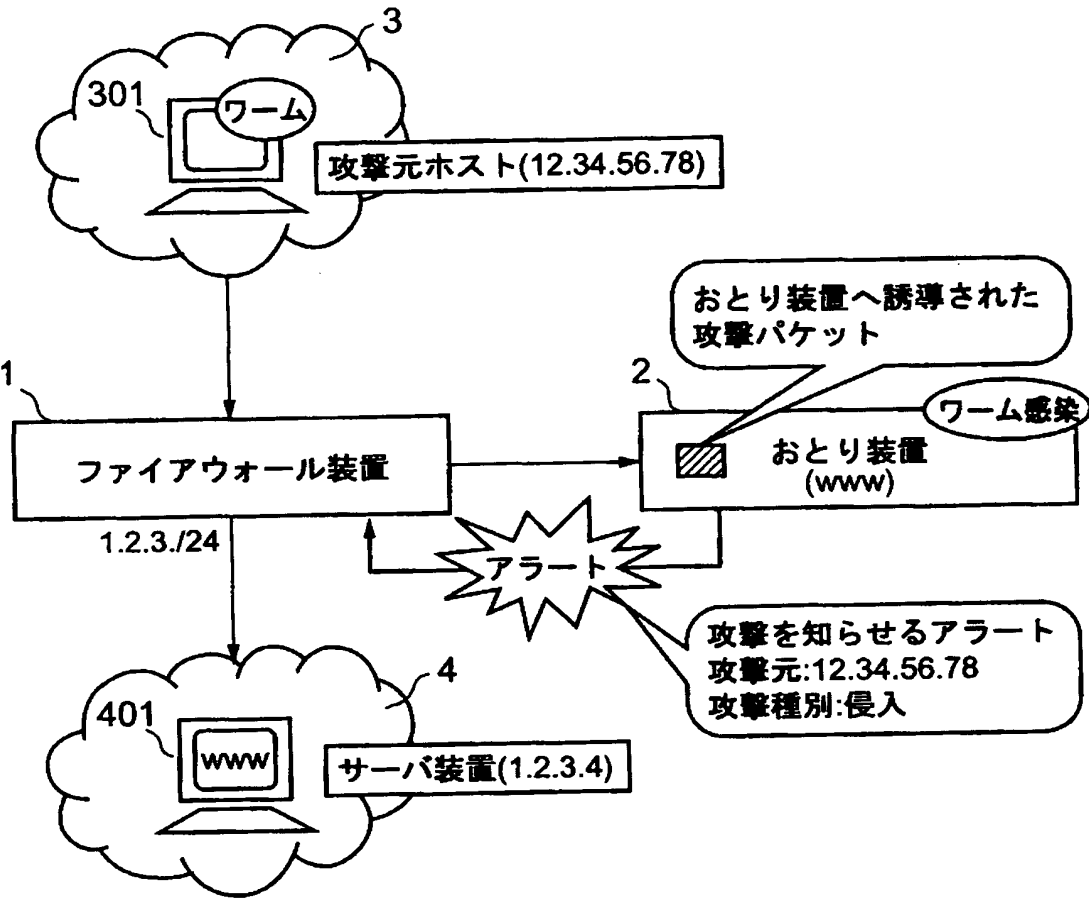
【図 9】



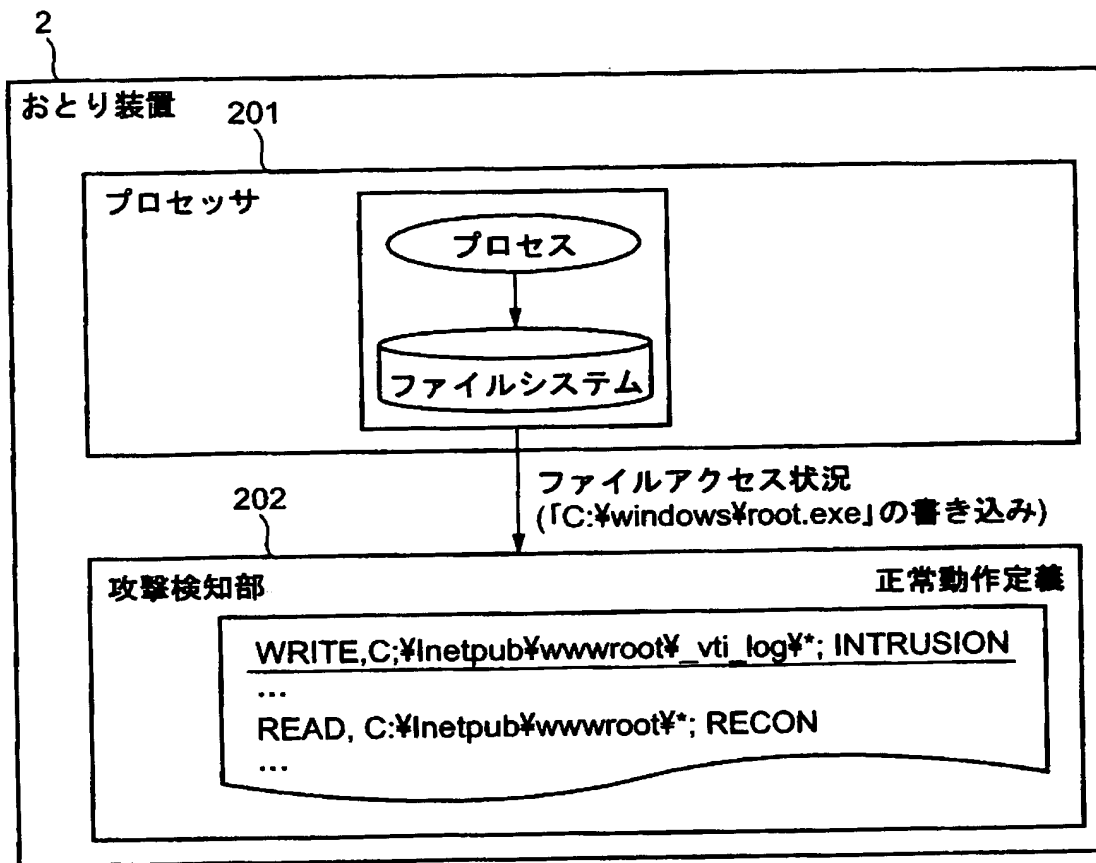
【図 10】



【図 11】



【図 12】



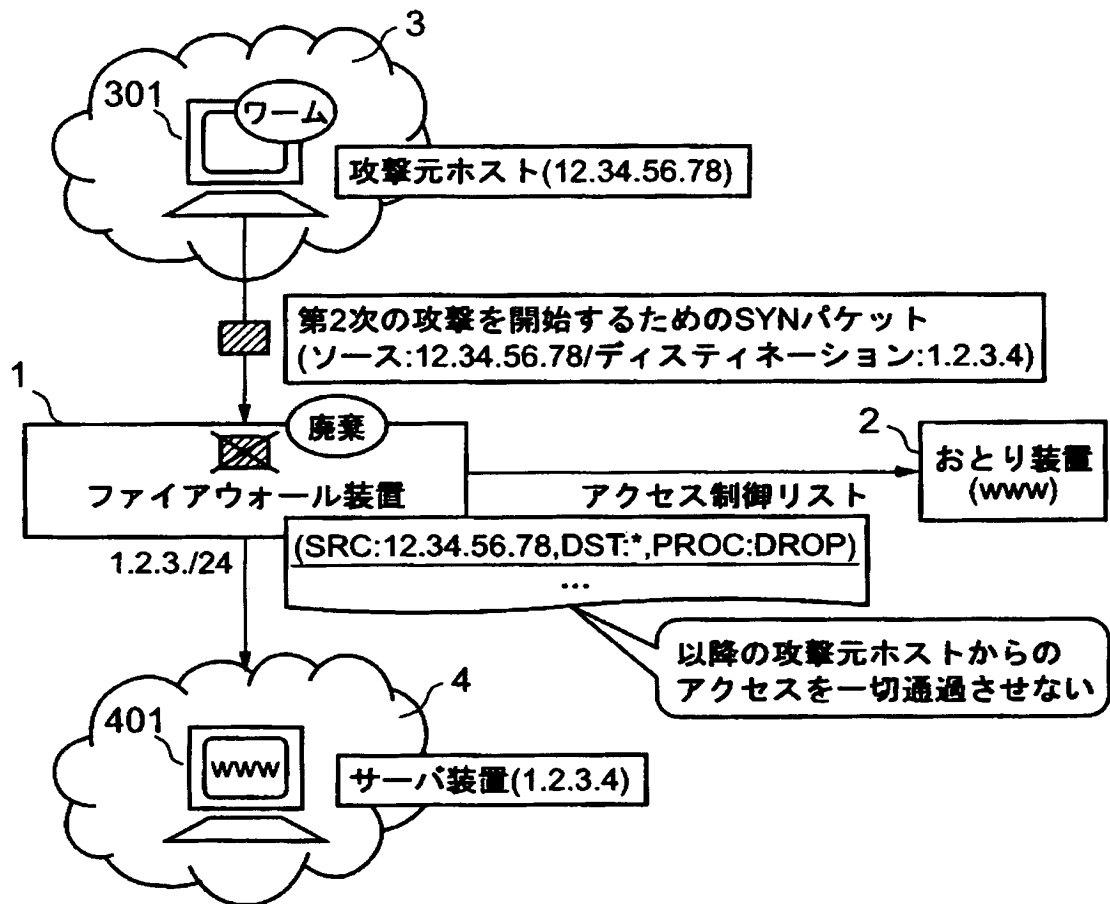
【図 13】

アクセス制御リストの更新

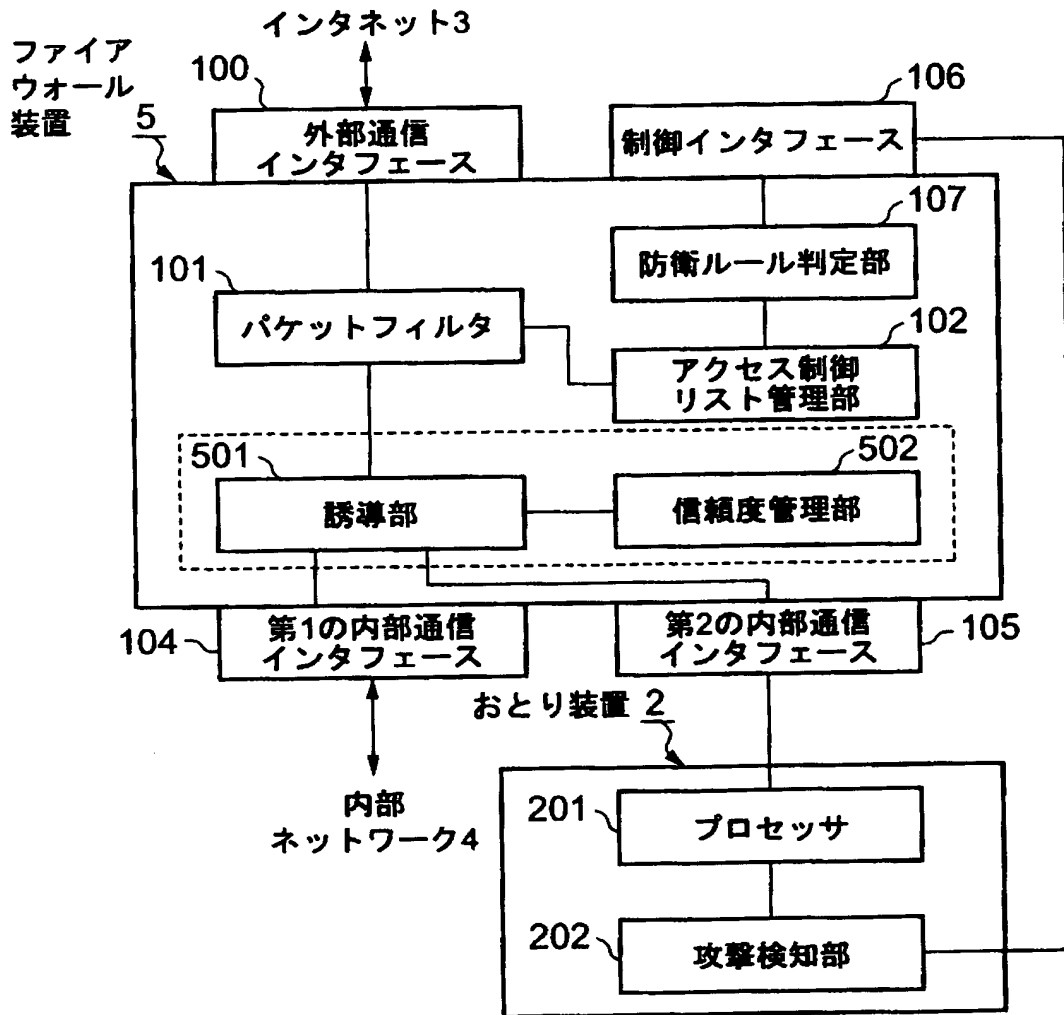
ソースIPアドレス (SRC)	デスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
12.34.56.78	*	DROP
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY



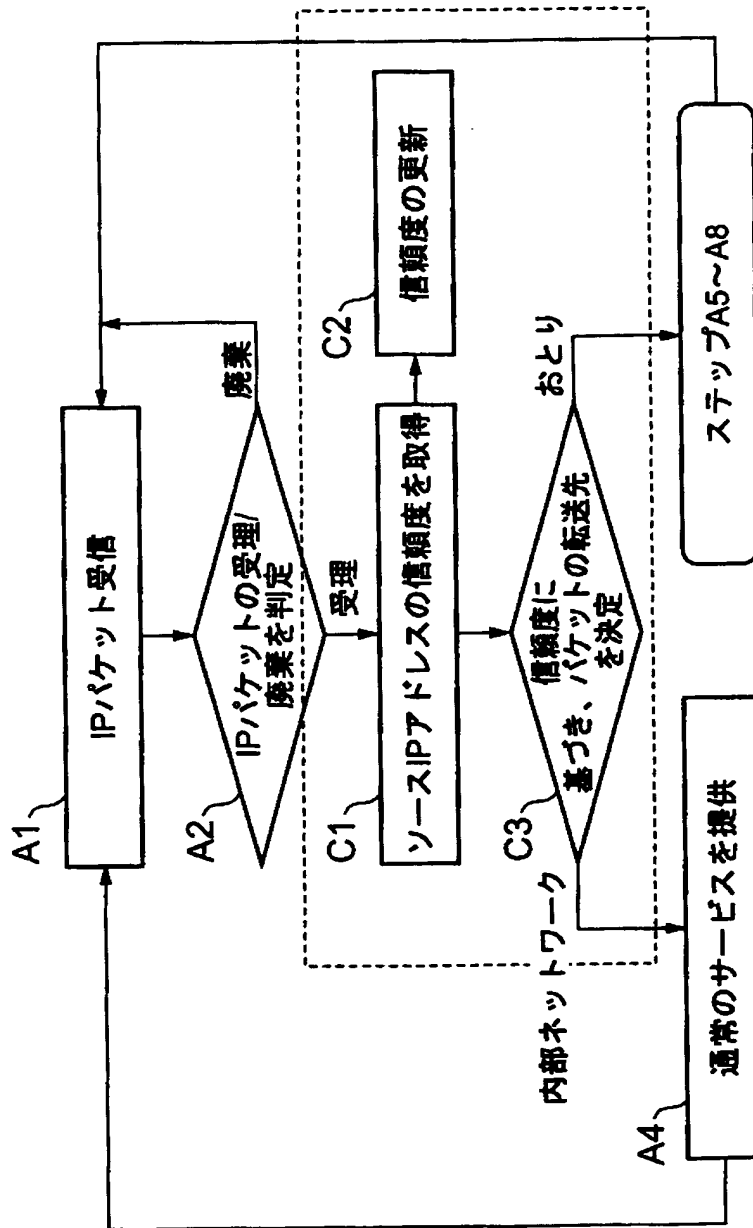
【図 14】



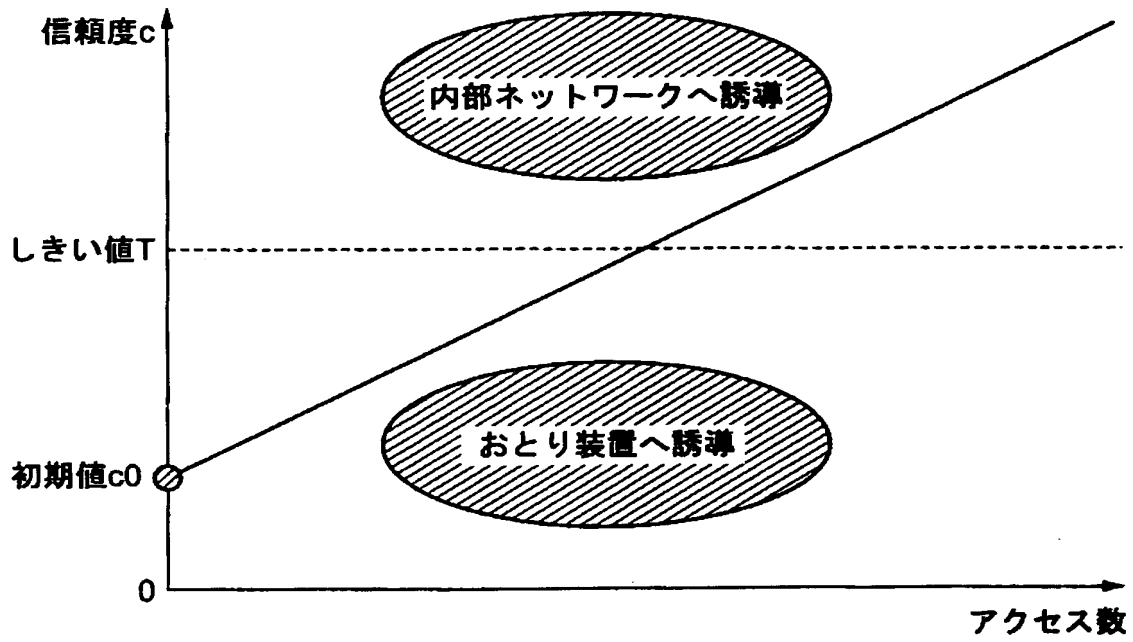
【図15】



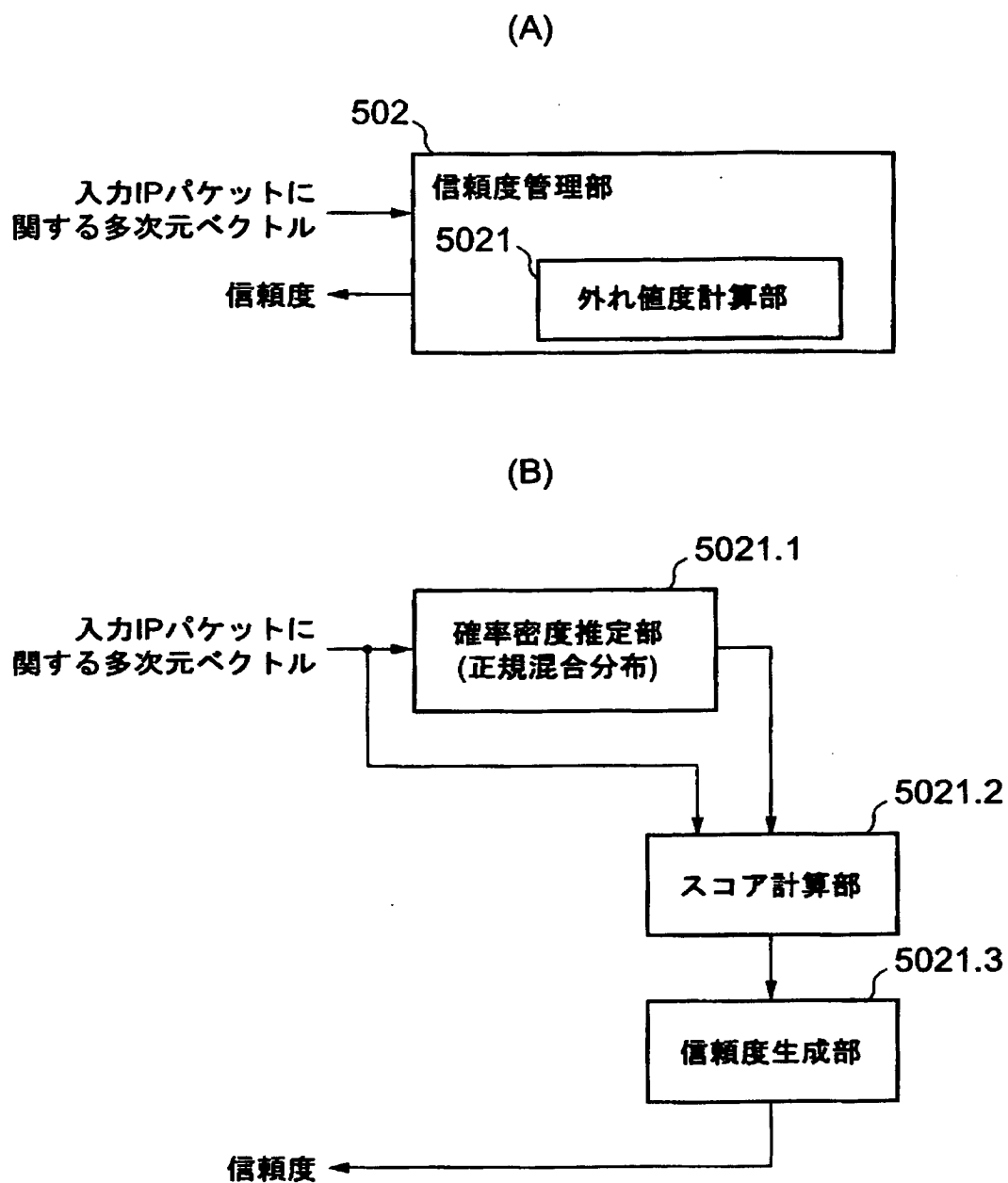
【図 16】



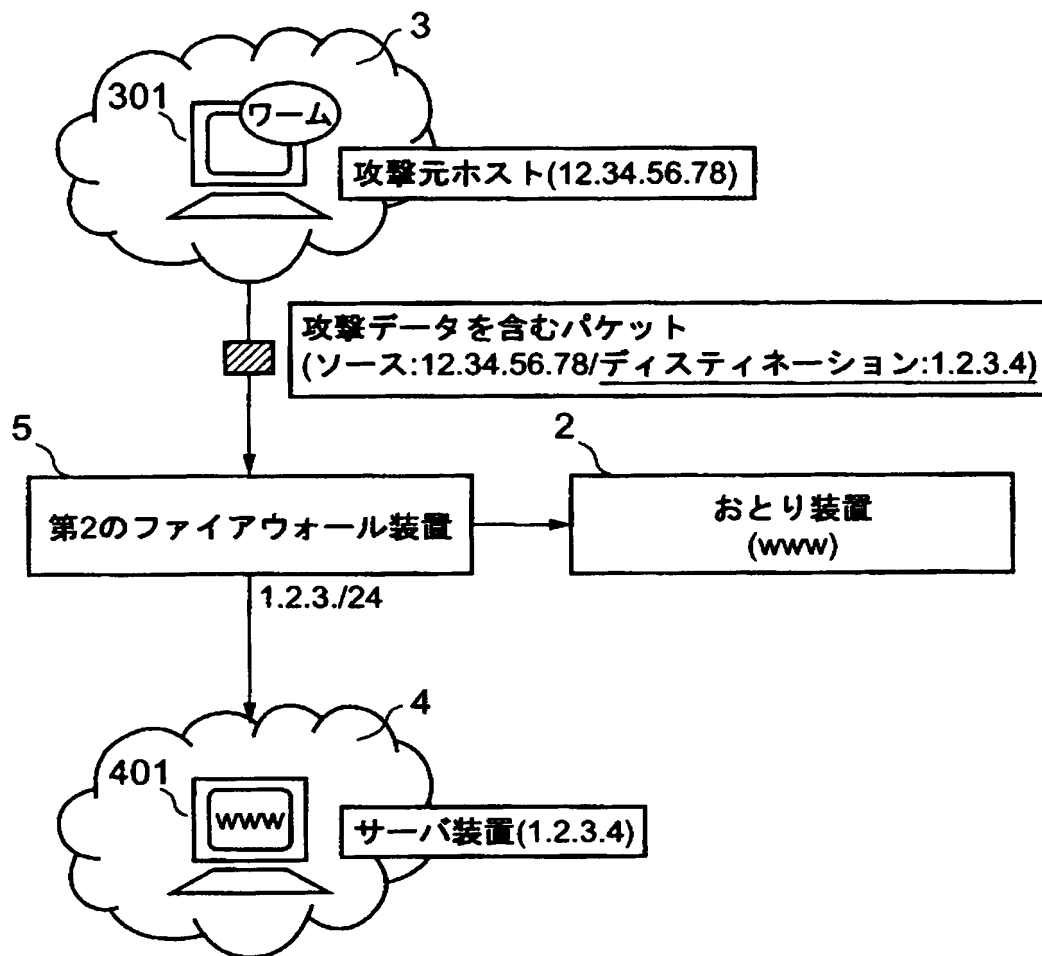
【図 17】



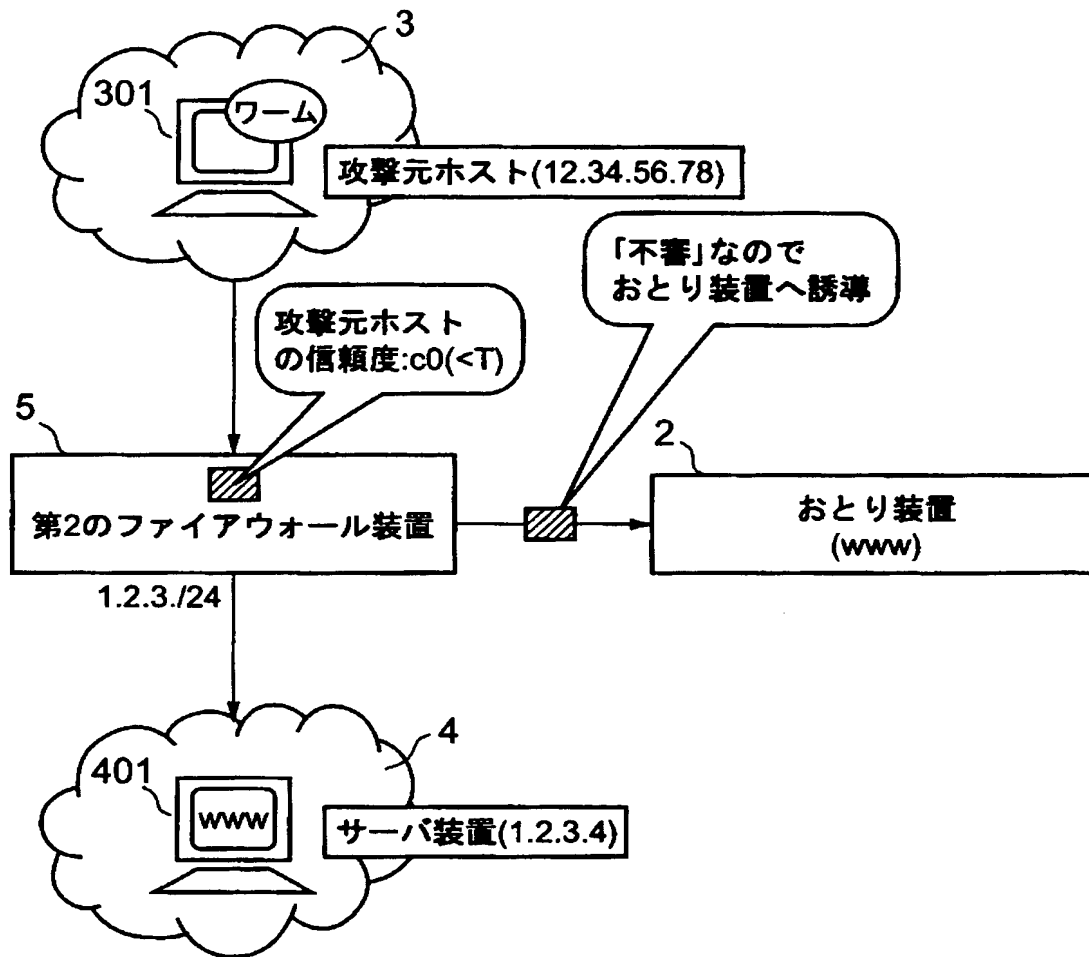
【図 18】



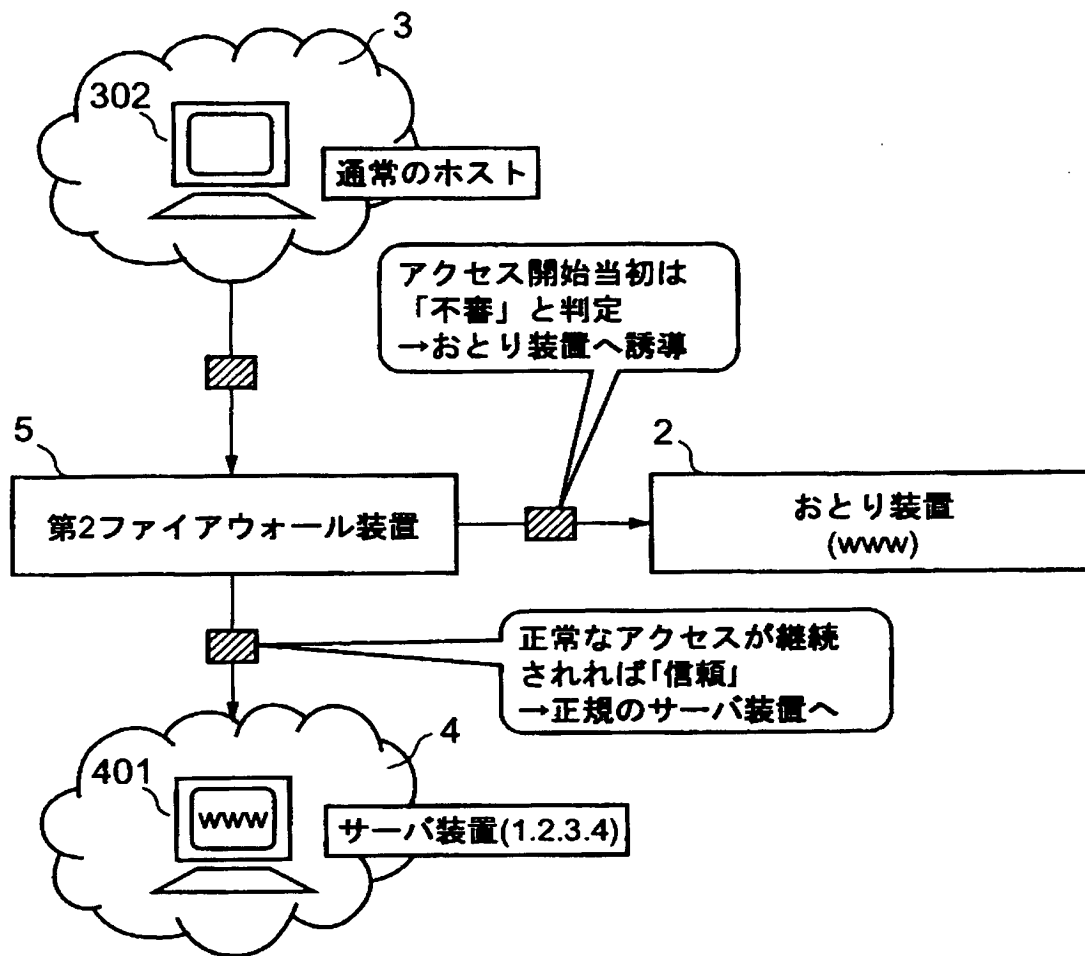
【図 19】



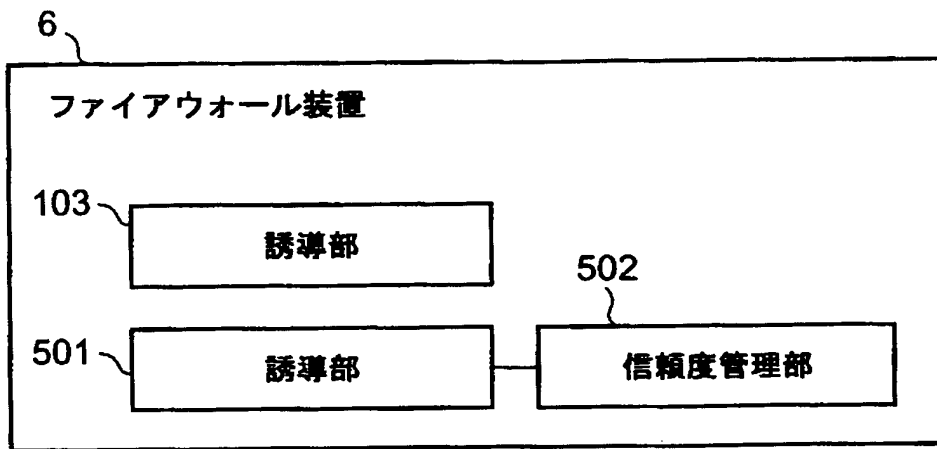
【図 20】



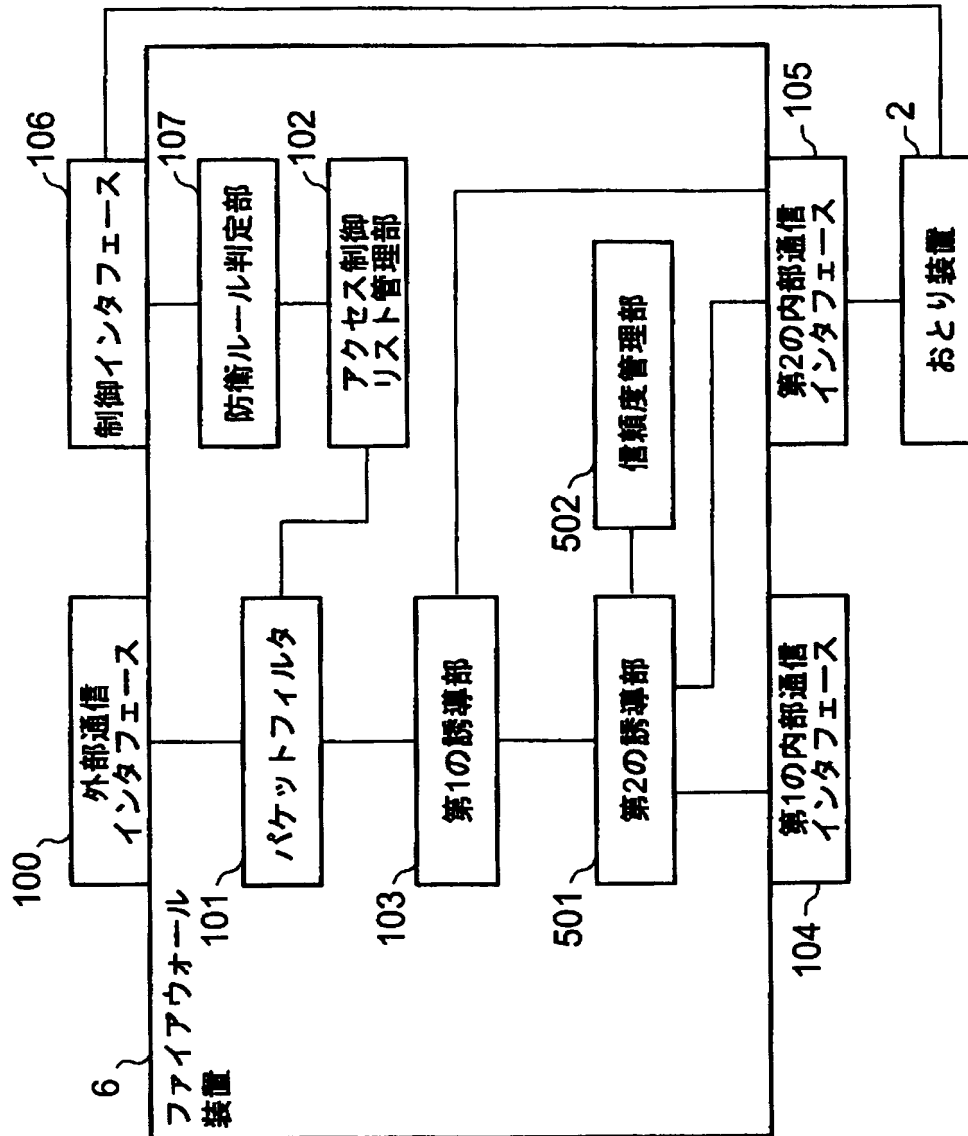
【図 21】



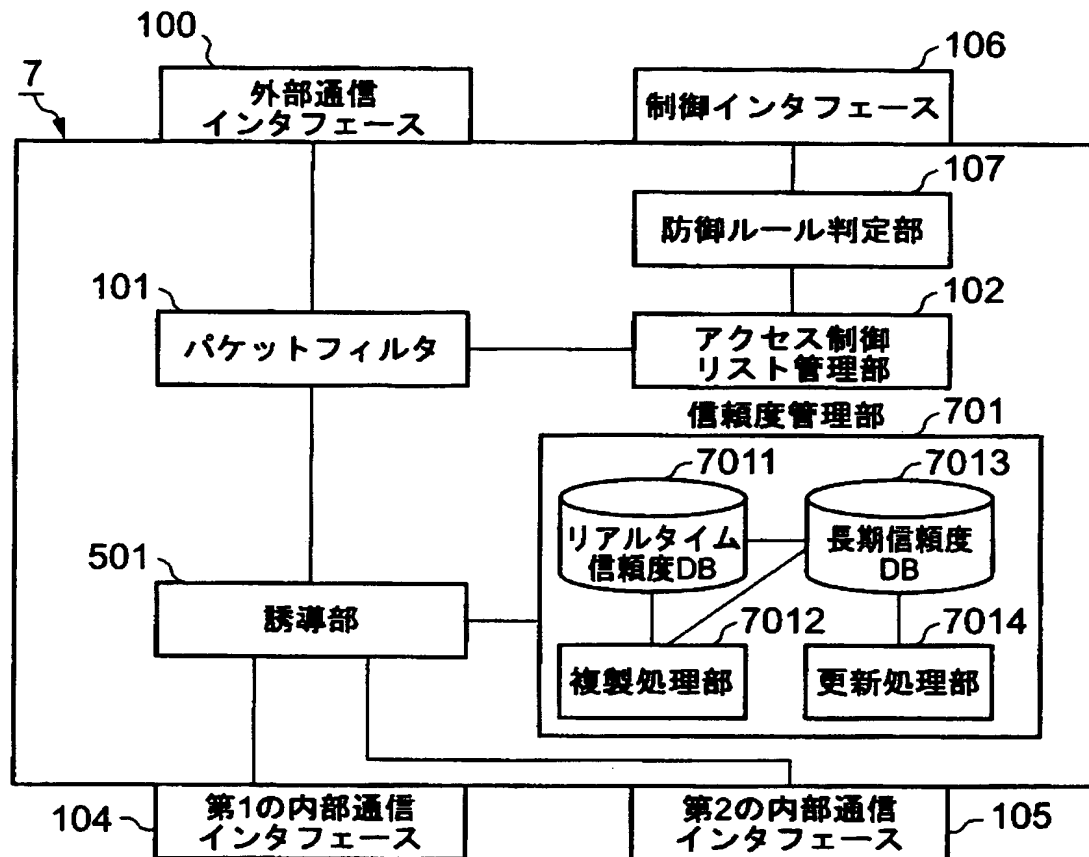
【図 22】



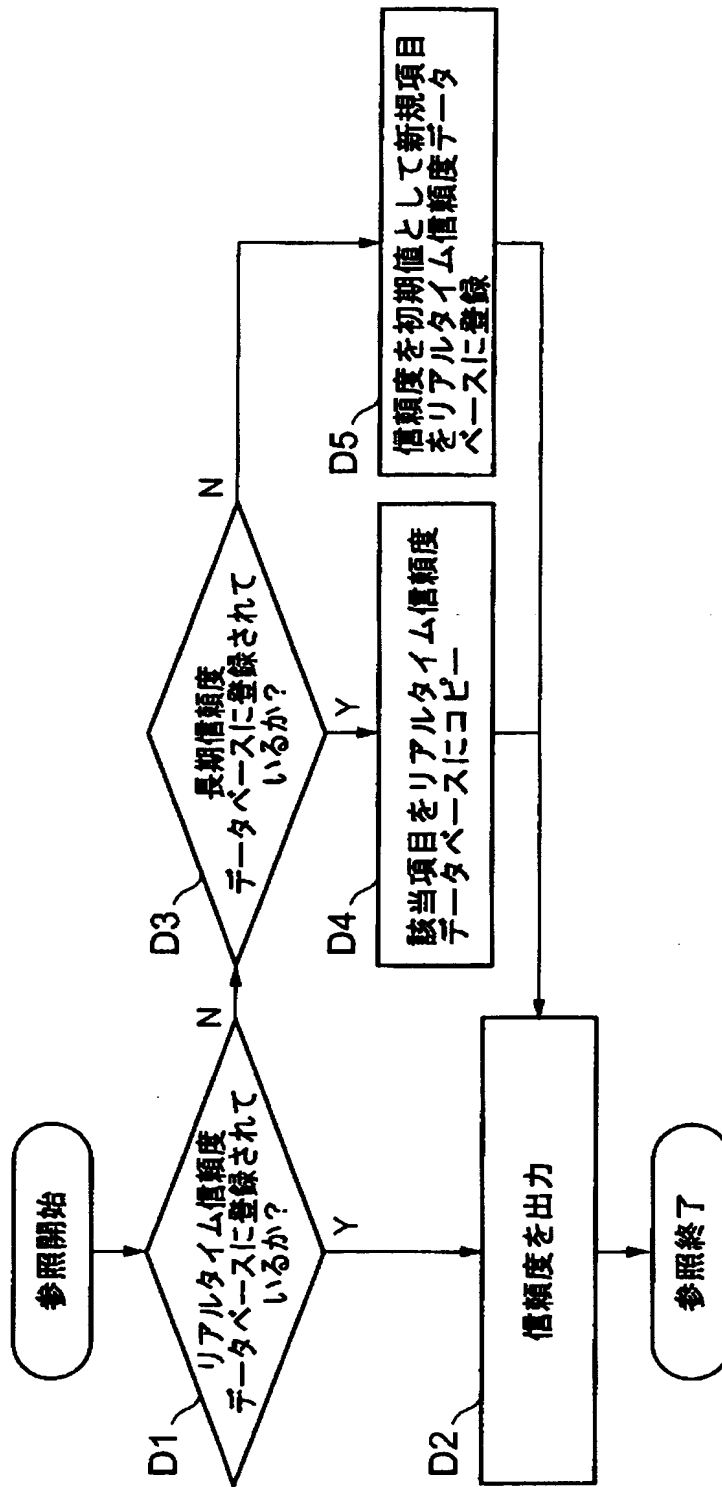
【図 23】



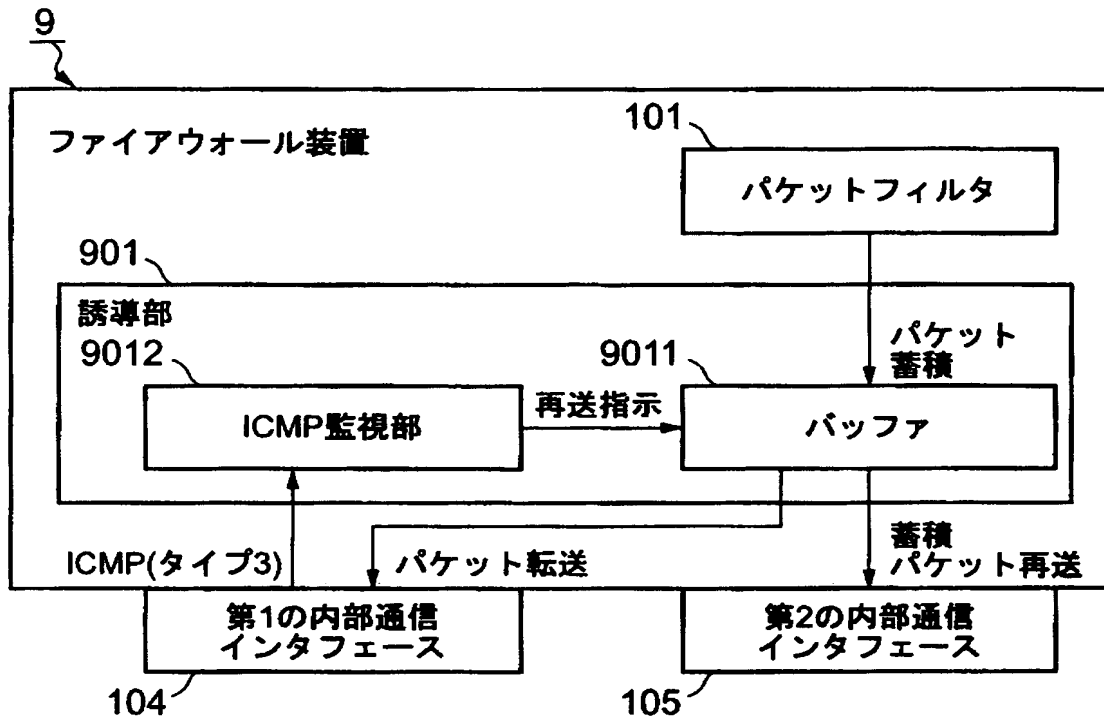
【図 24】



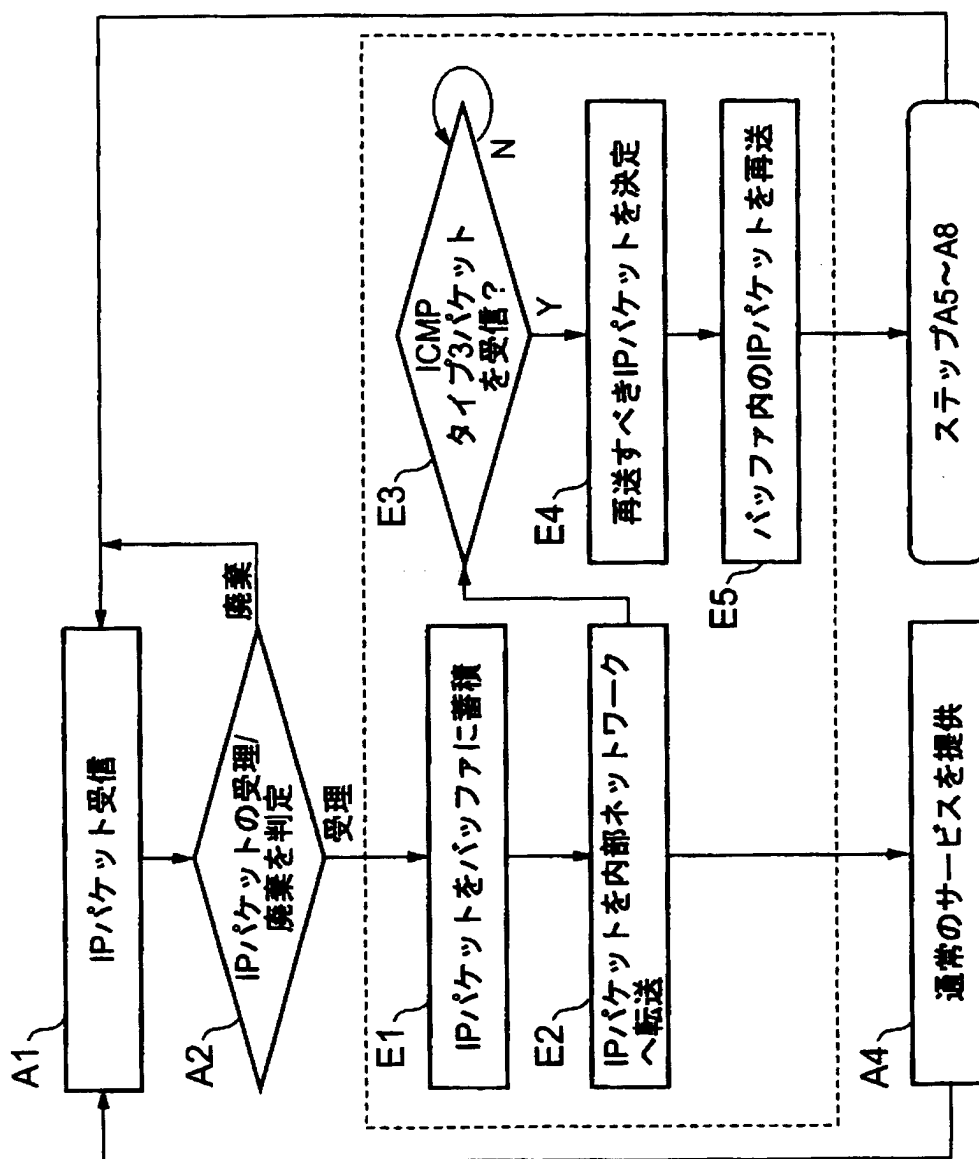
【図 25】



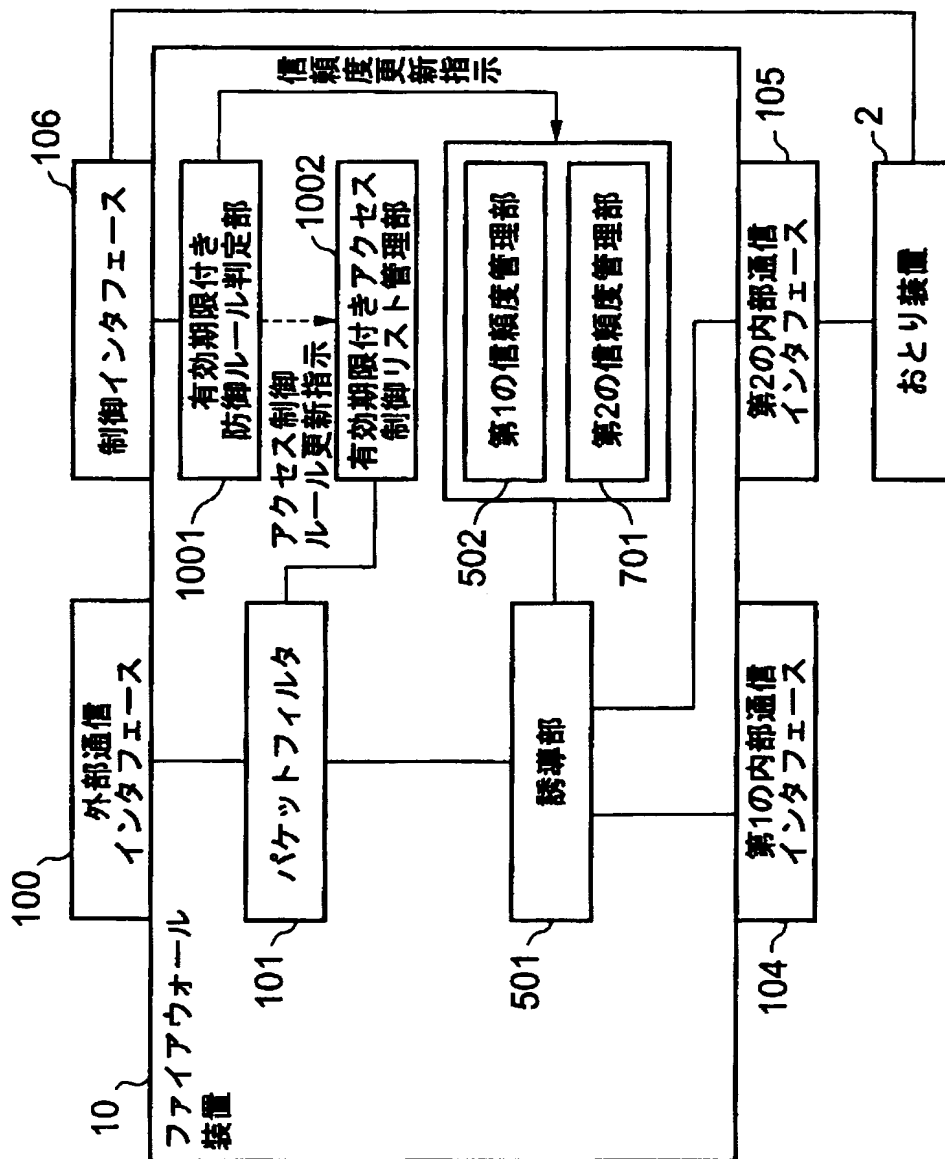
【図 26】



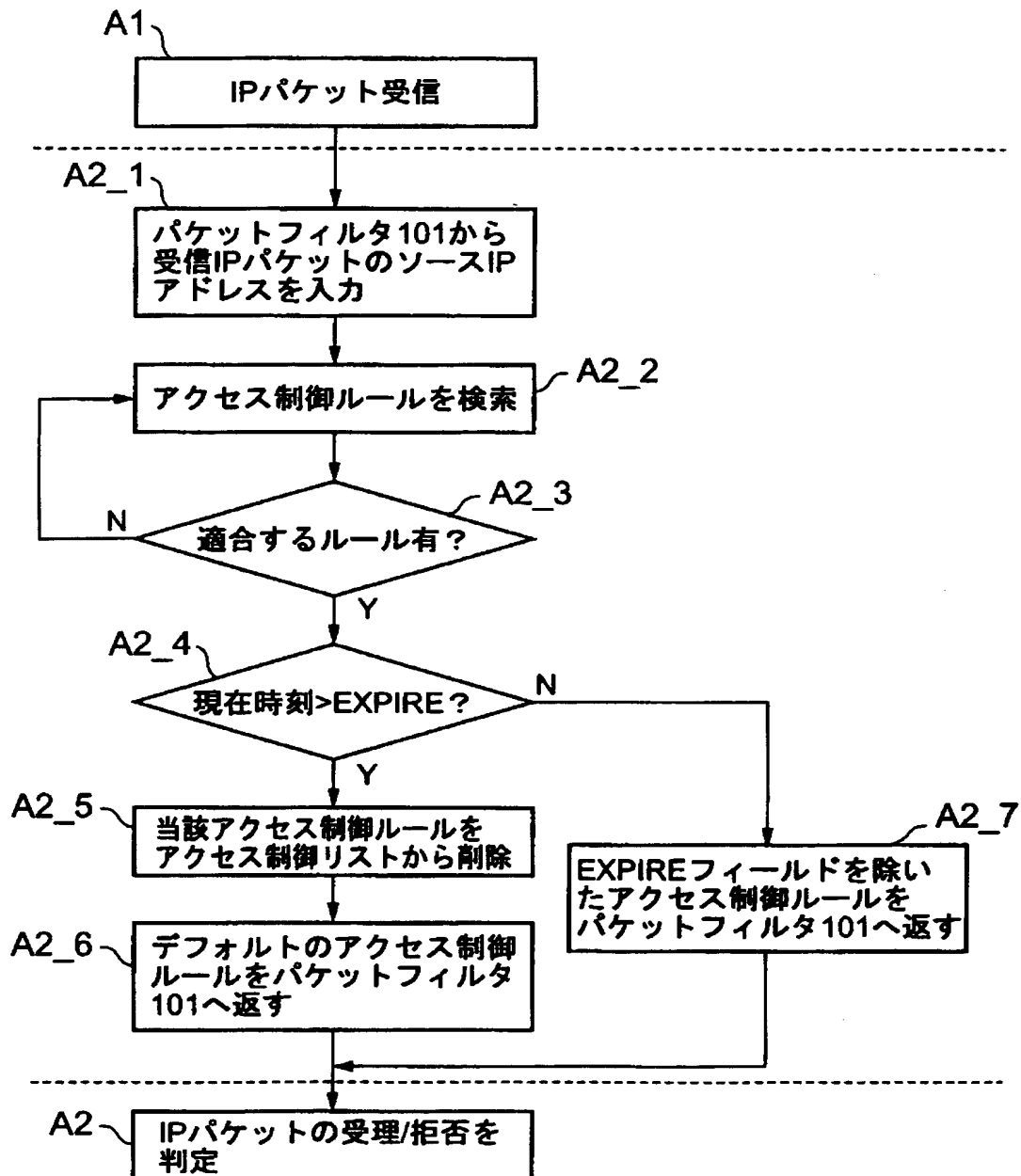
【図 27】



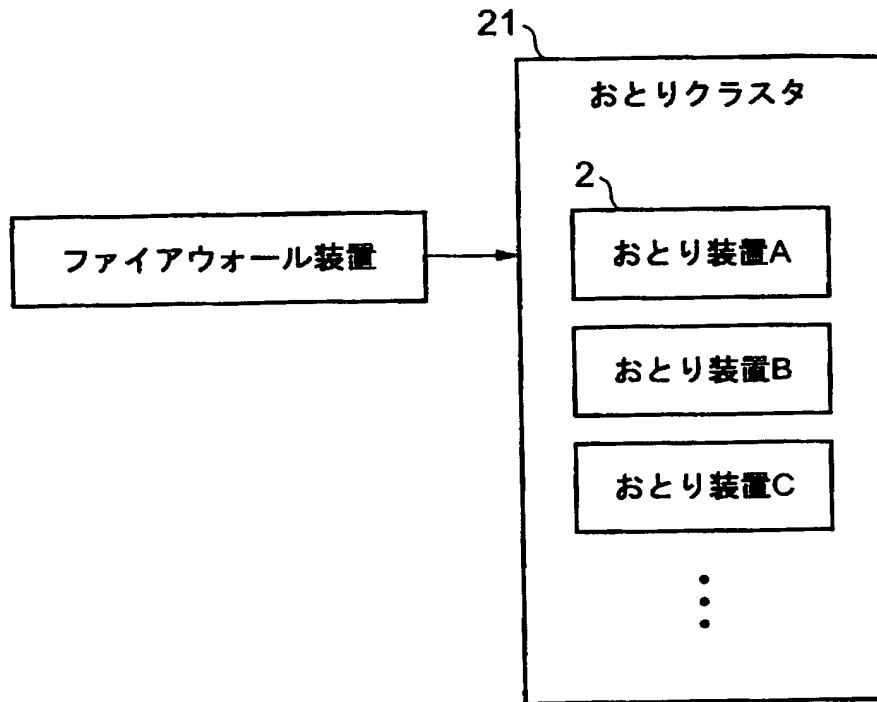
【図 28】



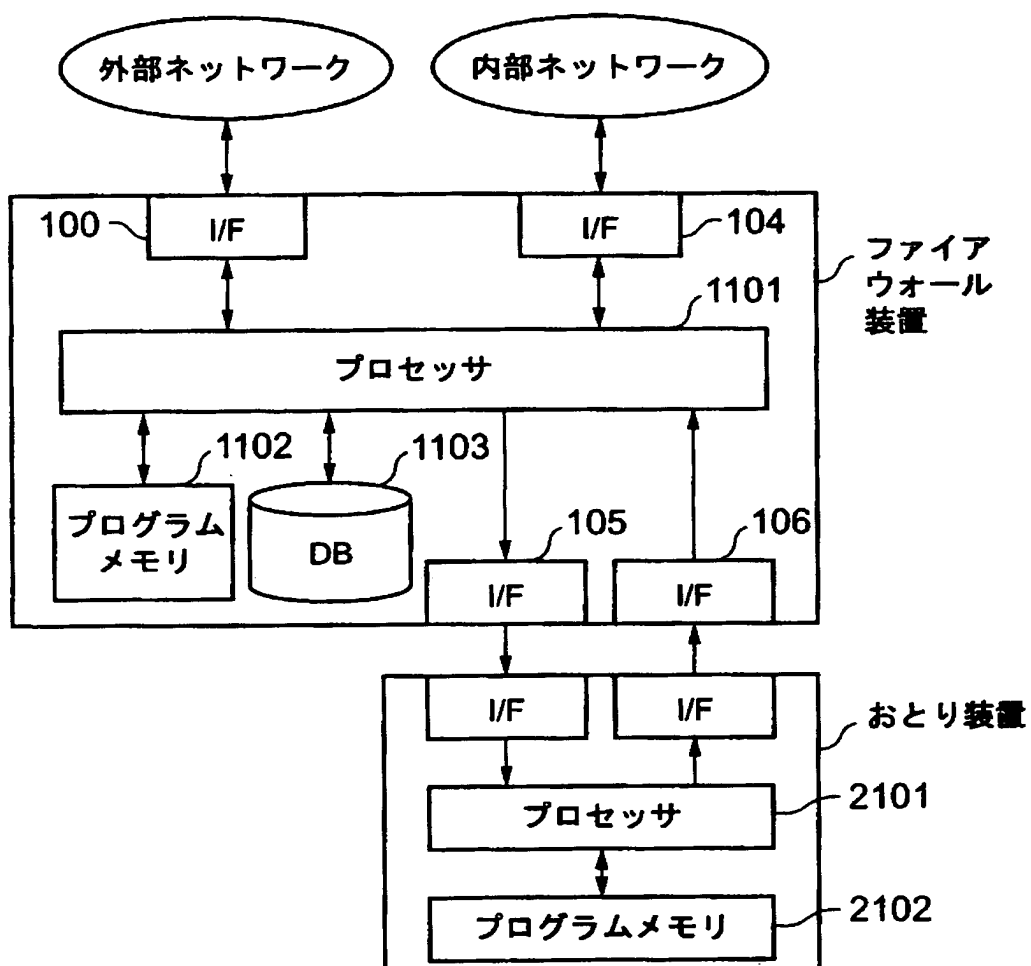
【図 29】



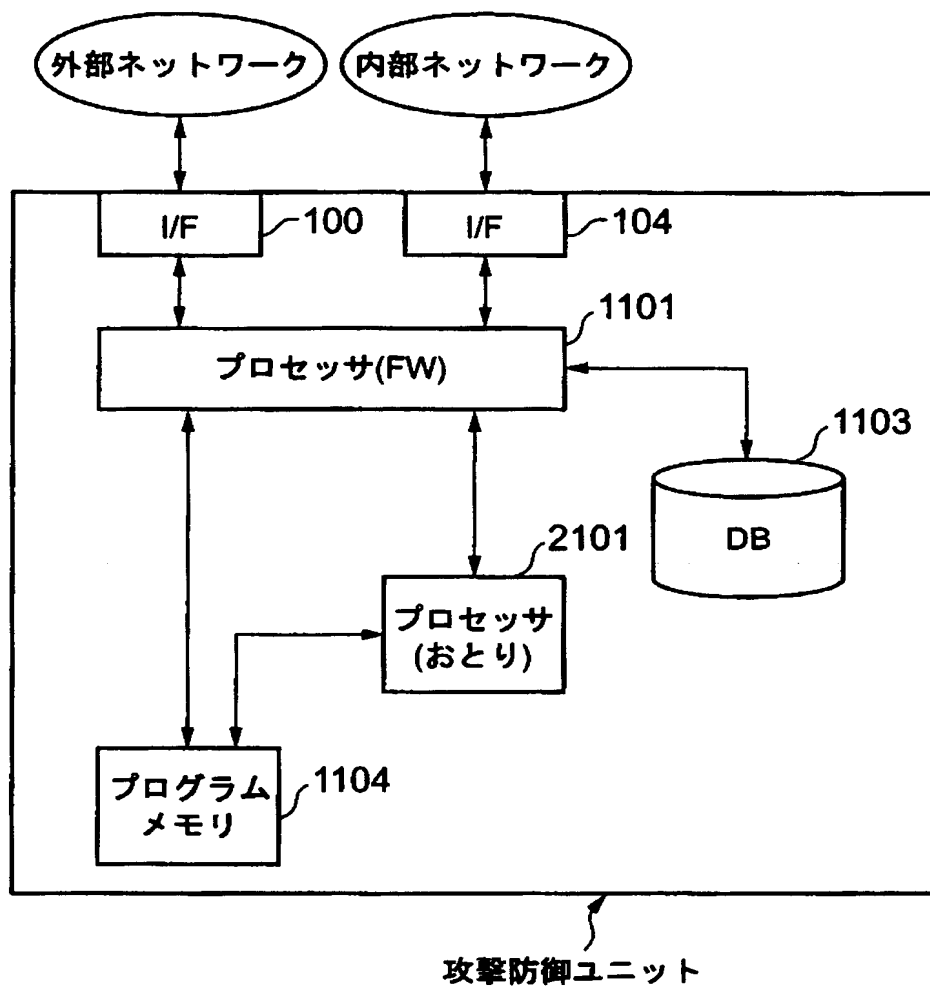
【図 30】



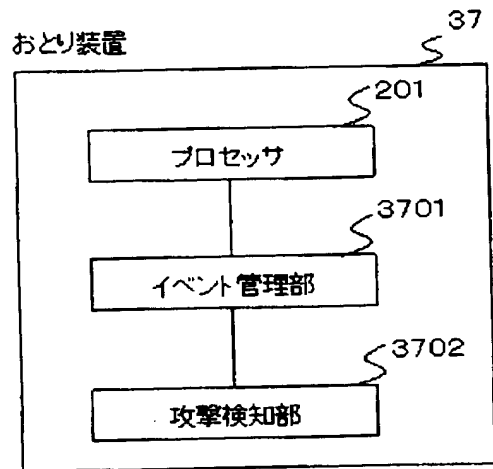
【図 31】



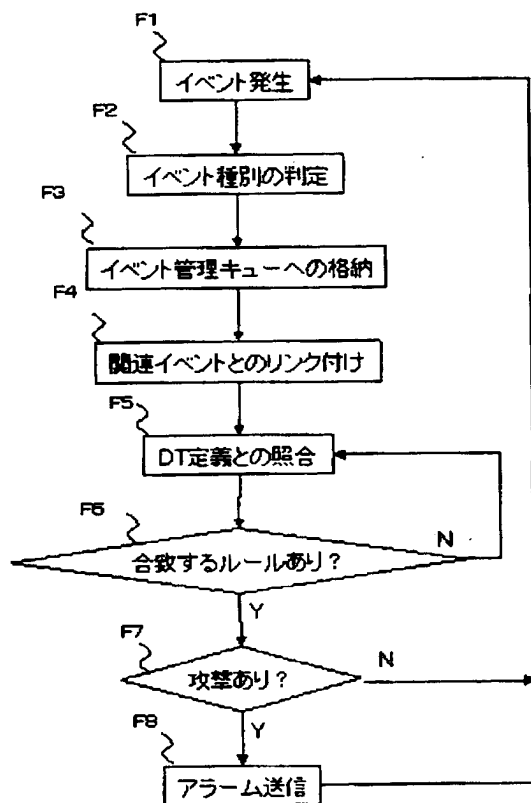
【図 3 2】



【図 33】



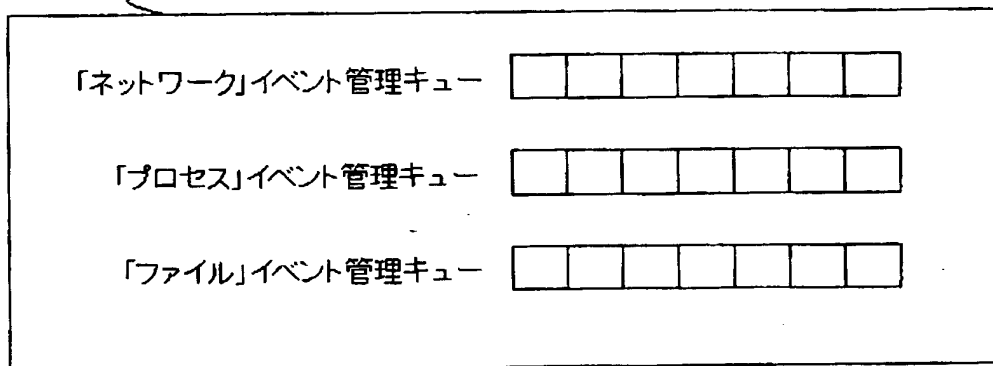
【図 34】



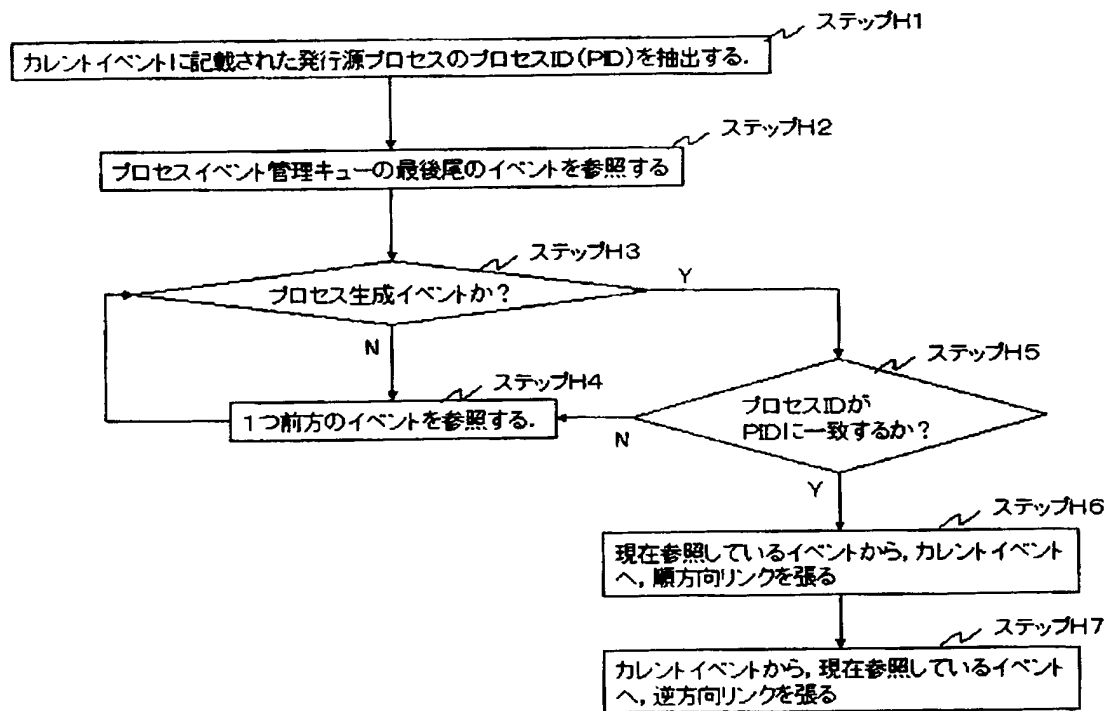
【図 35】

イベント名	イベント種別
PROC_EXEC	プロセス
PROC_FORK	プロセス
NW_ACCEPT	ネットワーク
FILE_OPEN	ファイル

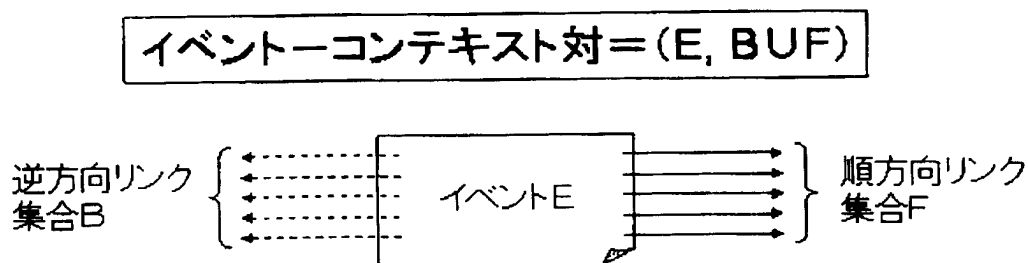
【図 36】

イベント管理部
3701

【図 37】



【図 38】



【図 39】

4101

DT定義ファイル

```

# (ルール1) WWWサーバによるログの書き出しを許可する。
0.0.0.0/0, <inetinfo.exe>, FILE_WRITE, C:\winnt\system32\LogFiles\*, ALLOW
# (ルール2) WWWサーバによるコンテンツ領域の読み込みを許可する。
0.0.0.0/0, <inetinfo.exe>, FILE_READ, C:\inetpub\wwwroot\*, ALLOW

# (ルール3) WWWサーバのサブシステムである登録CGIはデータベースを更新してよい。
0.0.0.0/0, <inetinfo.exe><regist.exe>$, FILE_WRITE, C:\data\client.db, ALLOW
# (ルール4) WWWサーバのサブシステムである出力CGIによるデータベース読み込みを許可。
0.0.0.0/0, <inetinfo.exe><view.exe>$, FILE_READ, C:\data\client.db, ALLOW

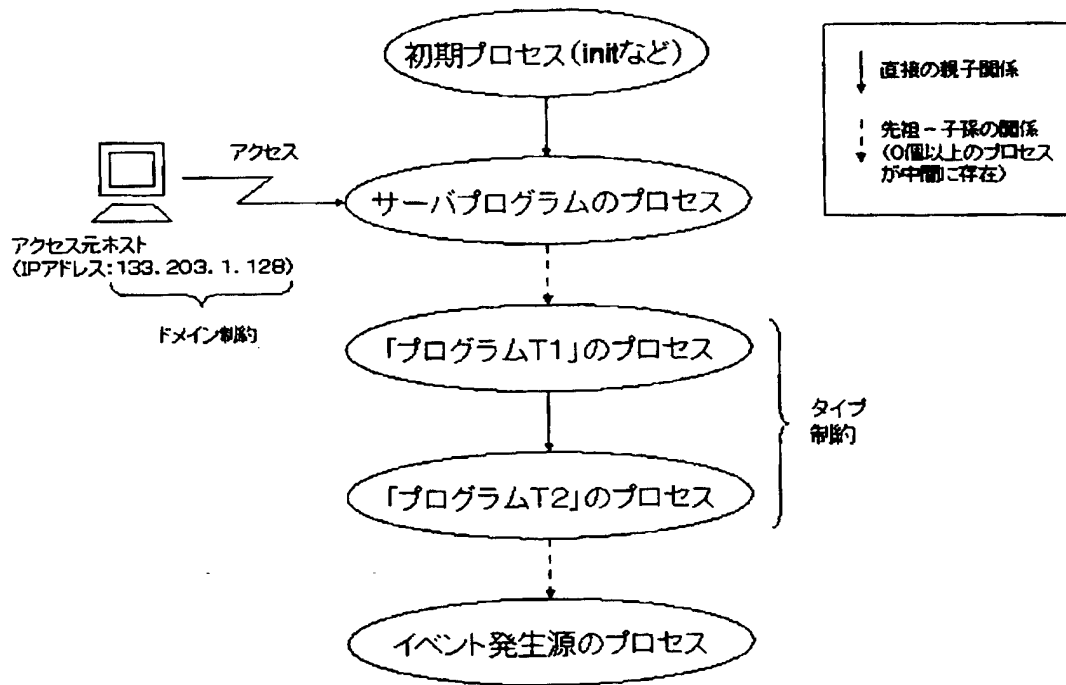
# (ルール5) FTPサーバはコンテンツ領域に書き出し可能
# ただし、管理者ドメイン10.56.192.0/24からのアクセスに限る。
10.56.192.0/24, ^<ftpd.exe>+$, FILE_WRITE, C:\inetpub\wwwroot\*, ALLOW

# (ルール6) WWWサーバは、特に許可されていない限り、ファイル書き出しを行わない。
0.0.0.0/0, <inetinfo.exe>, FILE_WRITE, *, DENY
# (ルール7) 許可されたプログラム以外によるデータベース領域のアクセスを禁止する。
0.0.0.0/0, *, *, FILE_READ|FILE_WRITE, C:\data\*, DENY
# (ルール8) 許可されたプログラム以外によるコンテンツ領域の書換えは攻撃である。
0.0.0.0/0, *, *, FILE_WRITE, C:\inetpub\wwwroot\*, DENY

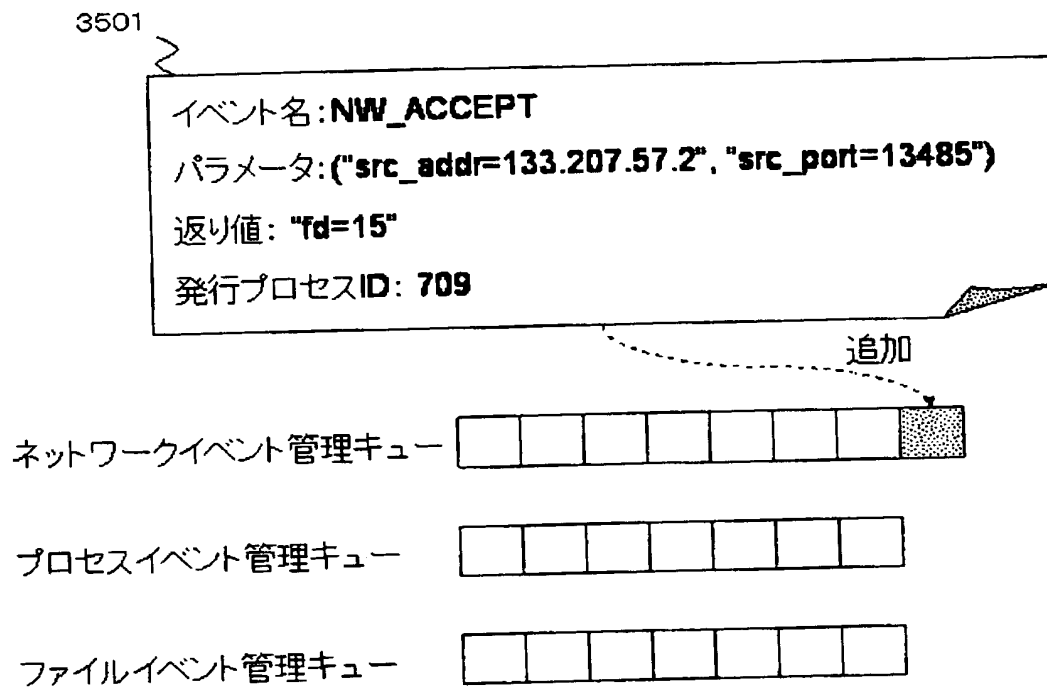
# (デフォルトルール) どのルールにもマッチしない場合は「許可」。
DEFAULT; ALLOW

```

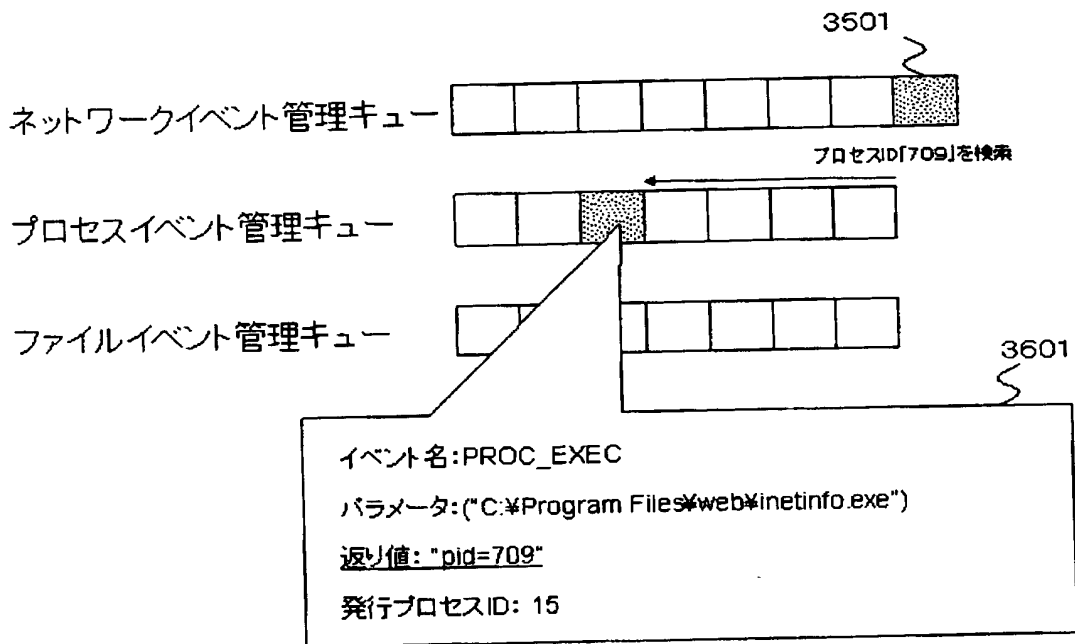
【図 40】



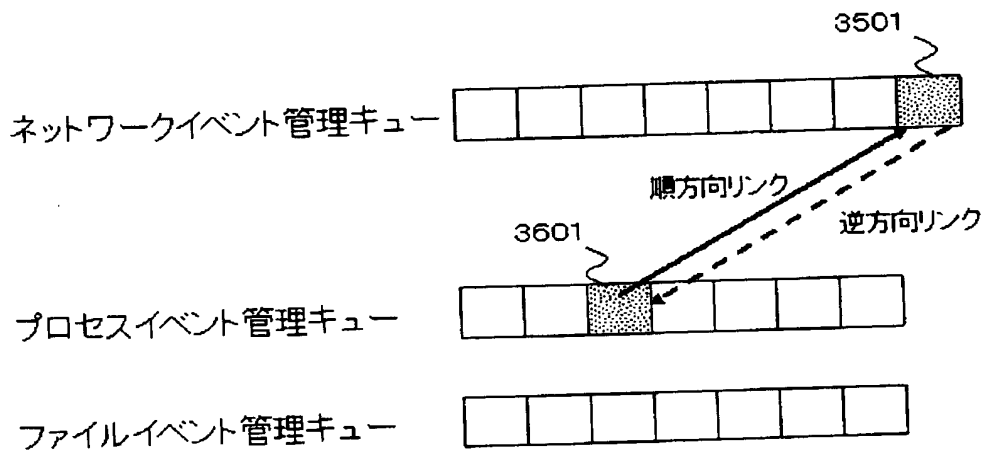
【図 4 1】



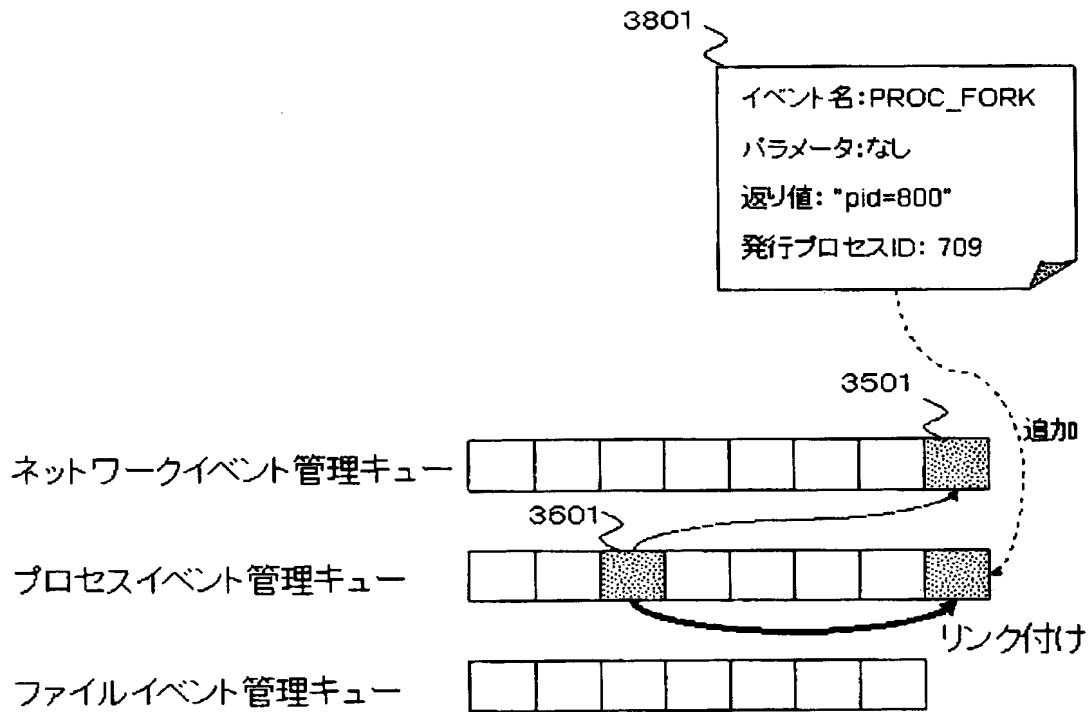
【図 4 2】



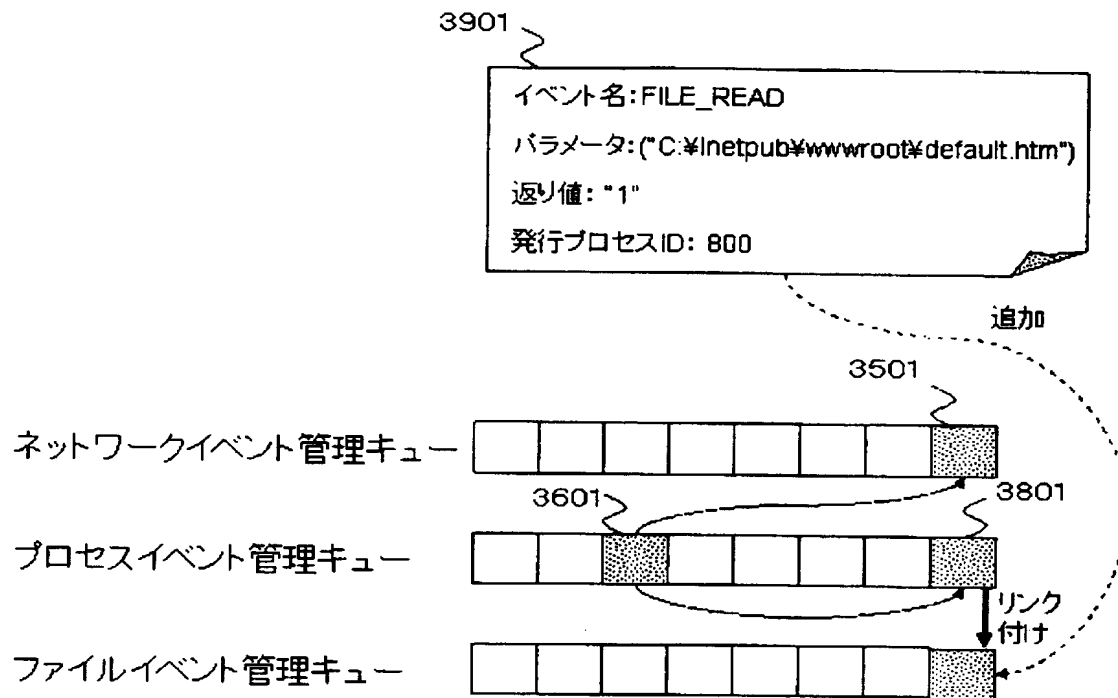
【図 4 3】



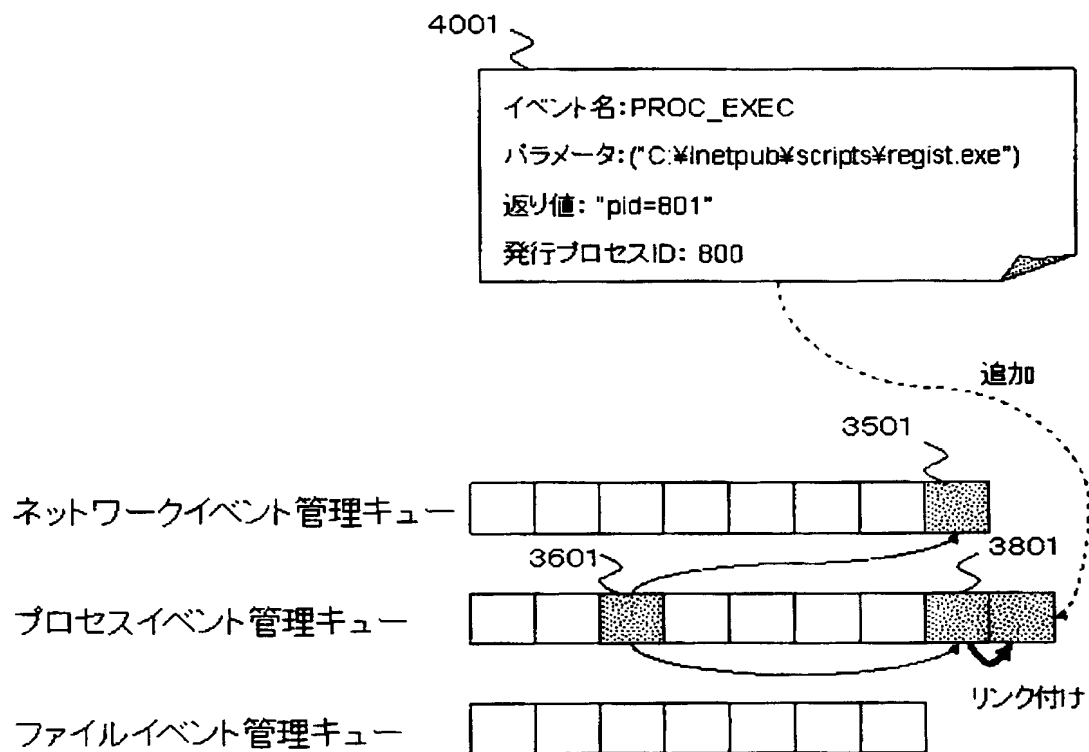
【図 4 4】



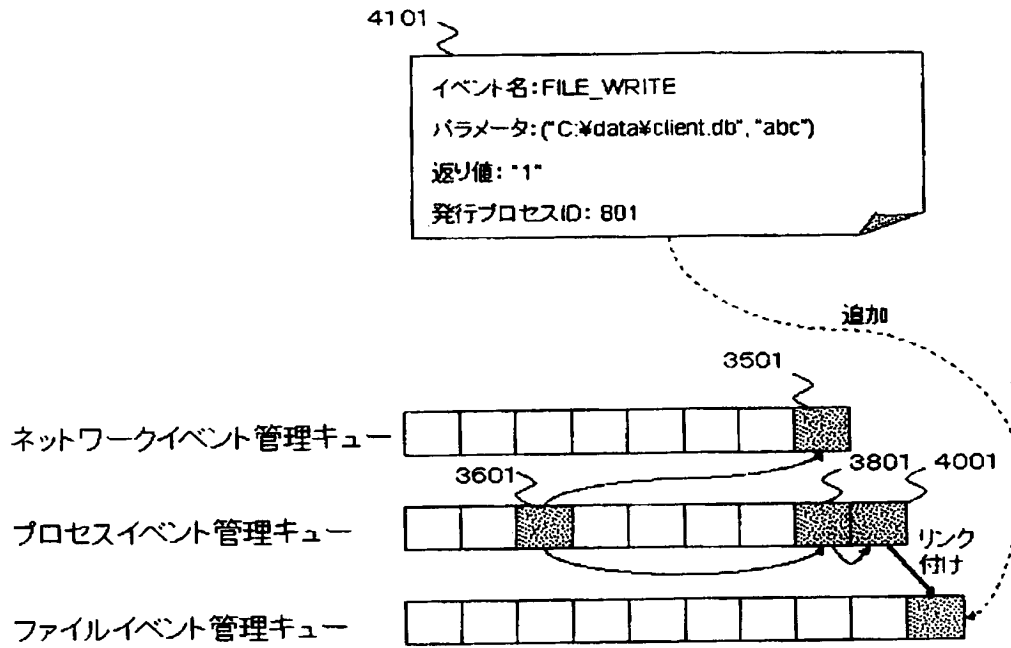
【図 4 5】



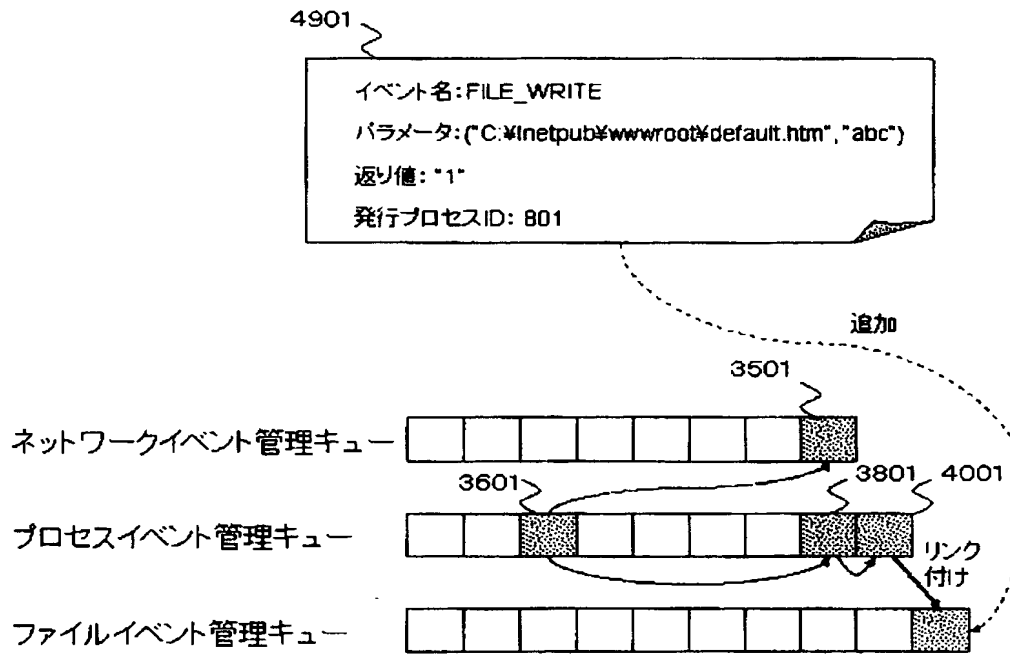
【図 4 6】



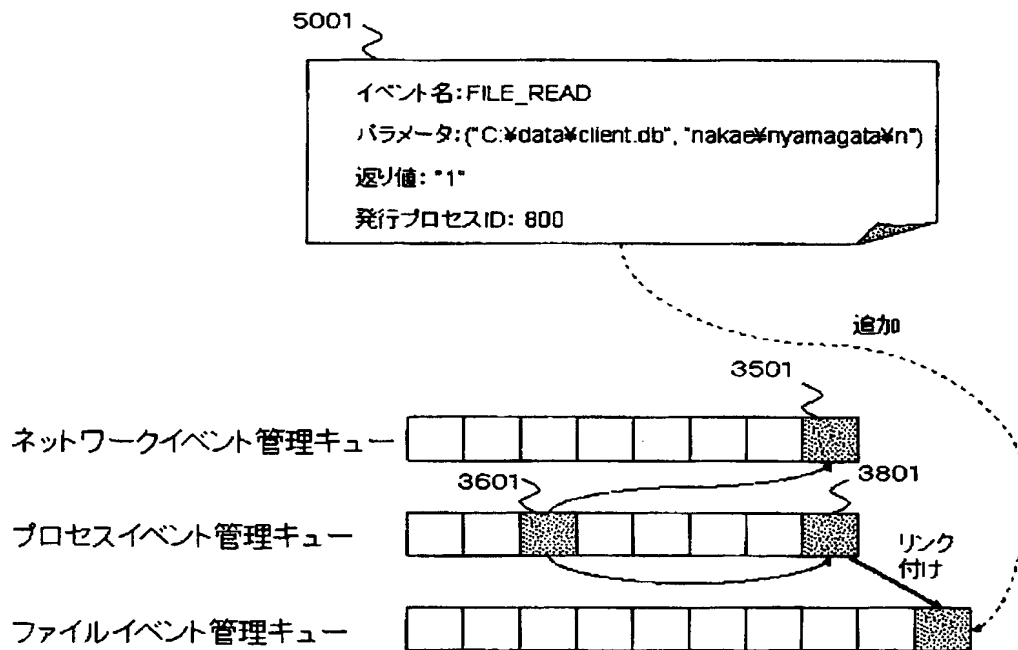
【図 47】



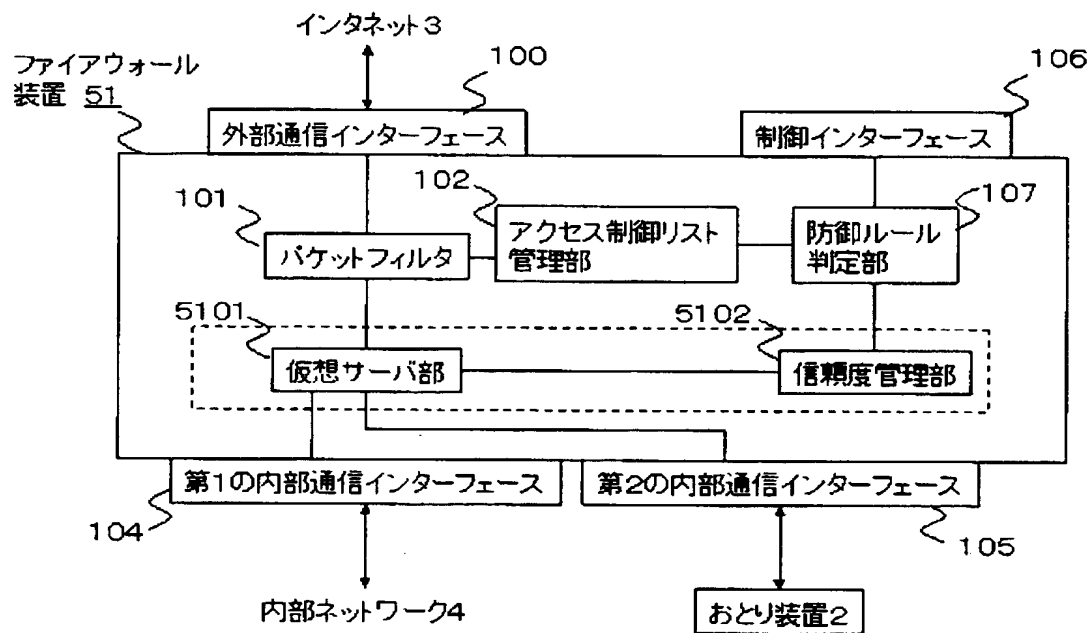
【図 4 8】



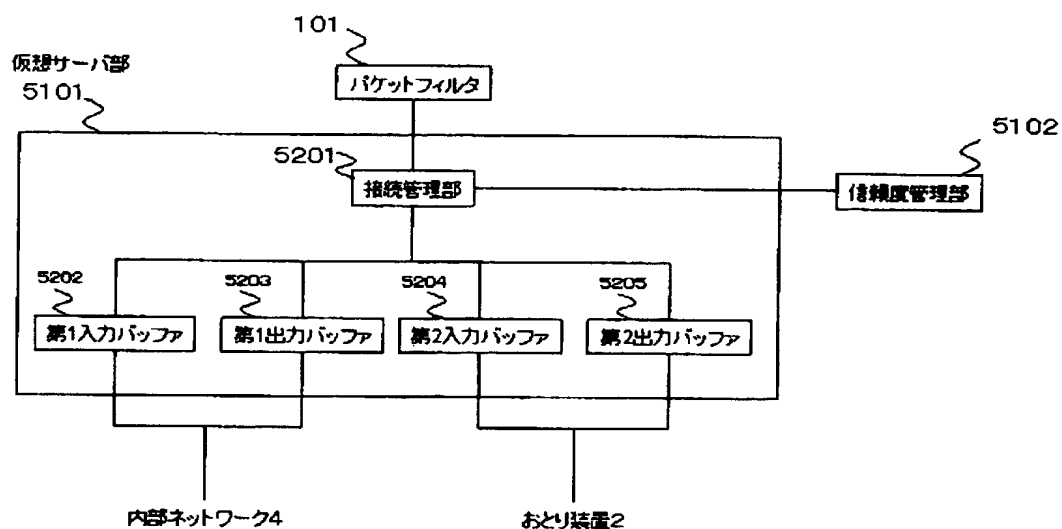
【図 4 9】



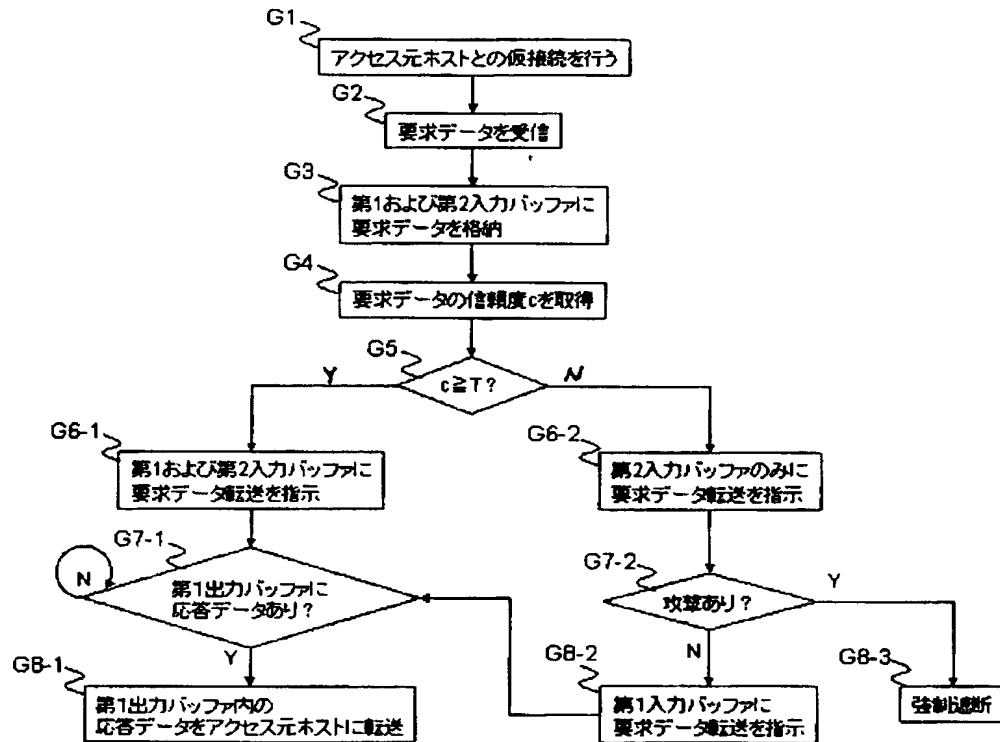
【図 50】



【図 51】



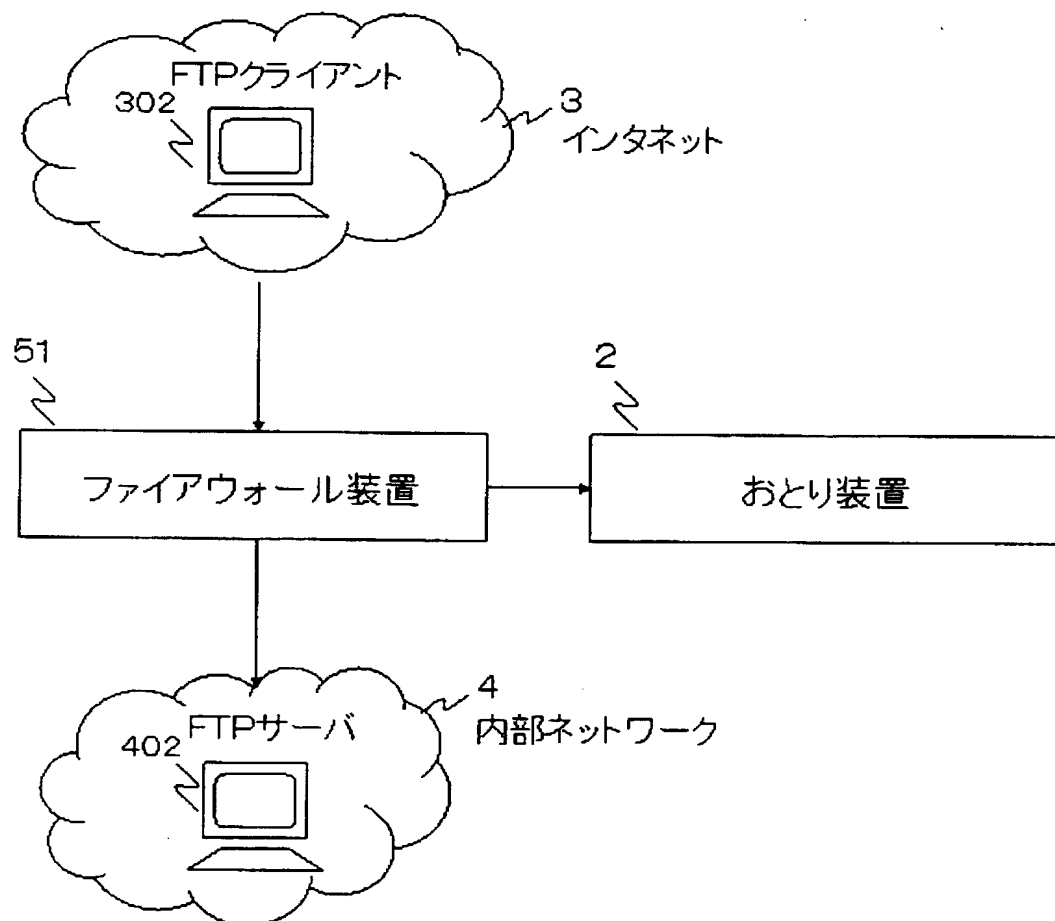
【図 52】



【図 5 3】

要求データ	信頼度
D0	1
D1	0
...	...
Dn	1

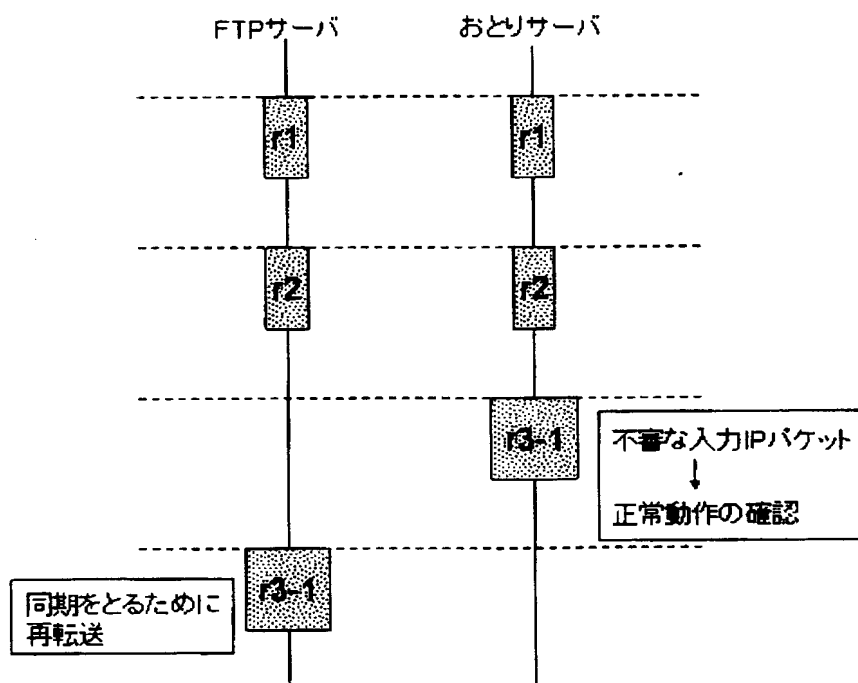
【図 54】



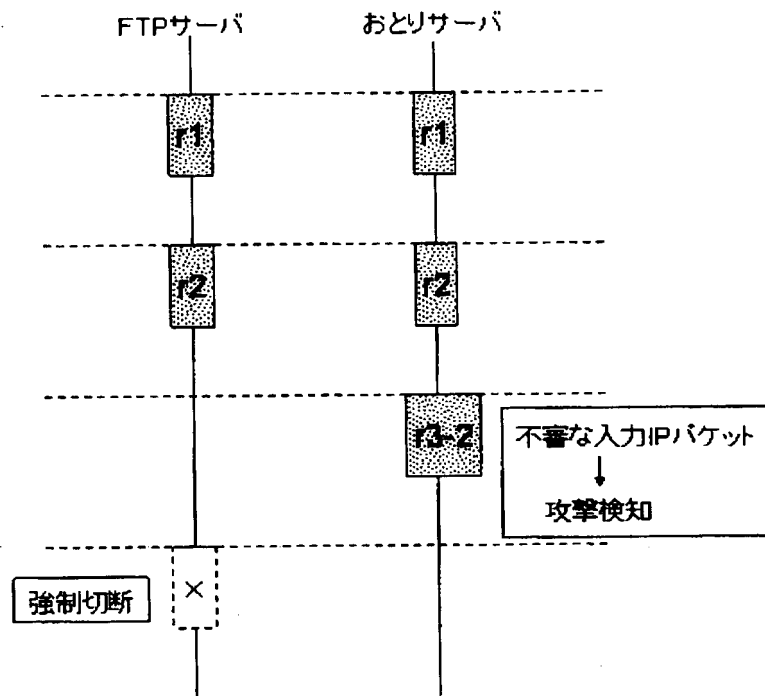
【図 5 5】

要求データ	信頼度
D0	1
D1	0
...	...
r1	0

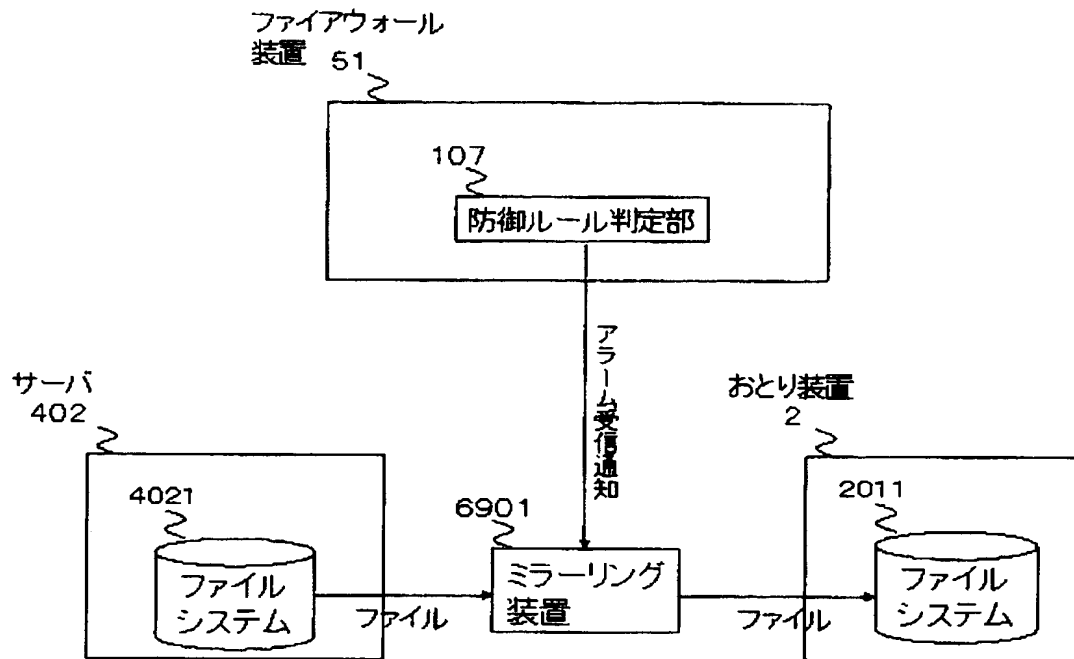
【図 5 6】



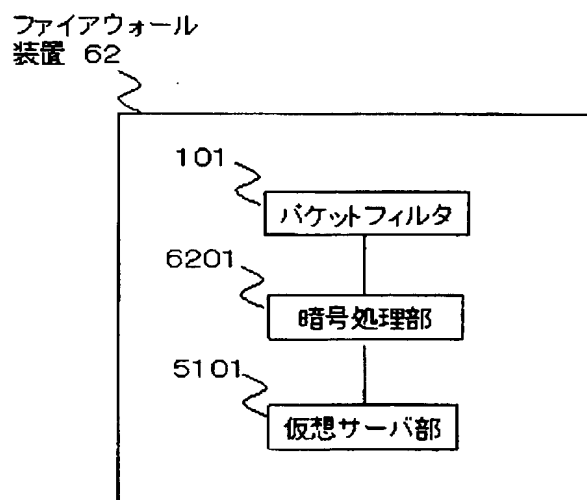
【図 57】



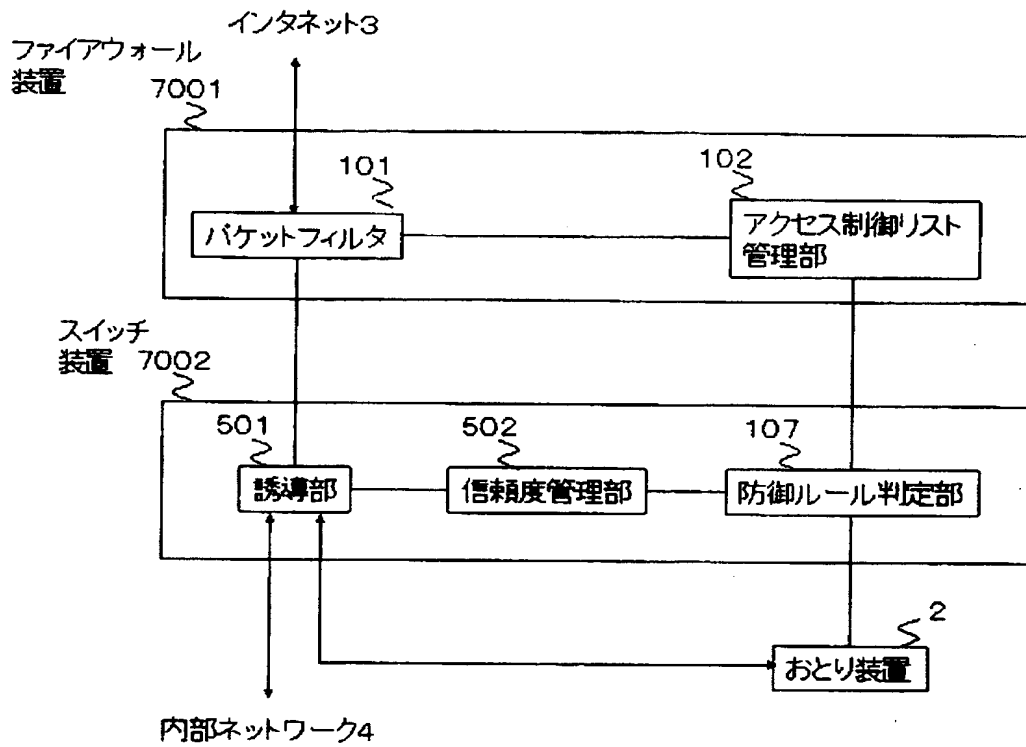
【図 58】



【図 59】



【図 60】



【書類名】 要約書

【要約】

【課題】 インターネットから内部ネットワークへのアクセスでSSLなど通信路暗号化技術が用いられた場合であっても不正なアクセスを検知し有効に防御する攻撃防御システム及び方法を提供する。

【解決部】 ファイアウォール装置1およびおとり装置2を備え、ファイアウォール装置1では、受け取ったIPパケットのヘッダ情報を参照し、所定のルールに基づいて攻撃の可能性がある「不審パケット」をおとり装置2へと誘導する。おとり装置2は、サービスを提供するプロセスを監視しながら、攻撃の有無を判定する。攻撃を検出した際には、攻撃元ホストのIPアドレスを含むアラートを生成してファイアウォール装置1に伝達する。当該アラートを受けたファイアウォール装置1は、以降、攻撃元ホストからのIPパケットの受入れを拒否する。

【選択図】 図2

特願 2003-074781

出願人履歴情報

識別番号

[000004237]

1. 変更年月日

1990年 8月29日

[変更理由]

新規登録

住 所

東京都港区芝五丁目7番1号

氏 名

日本電気株式会社